Smart Contract Technology and Financial Inclusion

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE

Fintech Note | No. 6

WORLD BANK GROUP

Ministry of Foreign Affairs of the Netherlands

BILL&MELINDA GATES *foundation*

Table of Contents

LIST OF BOXES

LIST OF FIGURES

LIST OF TABLES

Acknowledgments

ABBREVIATIONS AND ACRONYMS

AI	Artificial intelligence
AML	Anti-money laundering
CDD	Customer due diligence
CFT	Combatting the financing of terrorism
DAO	Decentralized autonomous organization
DLT	Distributed ledger technology
DFS	Digital financial services
FCP	Financial consumer protection
FATF	Financial Action Task Force
IoT	Internet of Things
MSME	Micro, small and medium enterprise
P2P	Peer-to-peer
RBA	Risk-based approach
SCF	Supply chain finance
SDD	Simplified due diligence
VASP	Virtual asset service provider
WBG	World Bank Group
WII	Weather index insurance

1.

BACKGROUND AND PURPOSE

FinTech Note No. 6 is part of a World Bank Group (WBG) series exploring the role of FinTech in economic development, with an emphasis on financial inclusion. In 2017, the WBG released FinTech Note No. 1, which investigates distributed ledger technology (DLT) and its possible development applications. This note picks up on a closely related innovation highlighted in FinTech Note No. 1, smart contract technology, which has received attention for its potential to facilitate a wide range of economic transactions. The note is geared toward local policymakers, who are analyzing FinTech developments for financial inclusion purposes, and WBG staff engaging with clients on financial inclusion projects.

Opinions vary considerably regarding smart contracts' projected role in the digital economy. While there are some feasible short-term smart contract use cases, smart contracts' widespread deployment will only accompany extensive uptake of DLT and blockchain. In this sense, smart contract usage is largely conditional on blockchain adoption. If blockchain ushers in a wave of decentralization in the financial industry, smart contracts will be embedded in a wide range of financial transactions.

Although blockchain optimism is strong, applications are incipient. In a 2019 survey of 1,386 senior executives from twelve countries, one global consulting firm found that over 80 percent of respondents believe a compelling business case exists for blockchain and that it will achieve mainstream adoption. However, the share of respondents who have actually initiated blockchain deployments decreased from 34 percent in 2018 to 23 percent in 2019. Consistent with the conditional relationship between smart contracts and blockchain, 95 percent of respondents see smart contracts as a highly or moderately important blockchain capability.

The purpose of this note is threefold. First, by bringing together in single resource key technological, economic, and legal aspects of smart contracts (sections 3-5), the note serves as a high-level reference on the basic elements of smart contracts. It equips local policymakers and WBG staff with the requisite foundation to effectively brainstorm about smart contracts' productive use in local economies.

Second, the note discusses select policy considerations (section 6) that local authorities, standard setting bodies, and international organizations will need to evaluate in order to ensure smart contracts' responsible and effective deployment

in retail and micro, small, and medium enterprise (MSME) finance. The note focuses on financial consumer protection, customer due diligence, key legal determinations, standardization and vetting, and data source automation.

Finally, the note analyzes smart contracts' potential applications in retail and MSME finance (section 7), focusing on supply chain finance, insurance, and consumer credit. It discusses the extent to which smart contracts could facilitate incremental financial inclusion gains and the changes they would introduce to these products. To this end, the Annex further examines the changes smart contracts could bring to two specific microfinance products, a weather index insurance policy and a mobile money-based, short-term unsecured loan.

2.

Key Takeaways

The table below outlines key takeaways from the analysis and maps them to relevant sections of the note. The takeaways are organized in two groups. The first group deals with smart contract applications and their financial inclusion implications. The second group catalogues select policy considerations for responsible and effective smart contract deployment.

Smart Contract Applications and Financial Inclusion Implications:	Sections
When paired with DLT, particularly blockchain, smart contracts potentially offer a transparent, automated, and efficient way to facilitate various contractual processes, especially monitoring the performance of agreements with less reliance on third parties.	3.3, 4, 7
Blockchain-based smart contracts could unlock value for firms and consumers through automation, self-execution, immutability, and distributed access and verification.	4, 7
Smart contracts are well-suited to capture certain operational contract clauses expressed in straightforward conditional logic but will struggle to express non-operational elements and those involving judgement or discretion. Smart contracts may also fundamentally alter or render unnecessary some common contractual elements.	5.2, Annex
Where process frictions and operational, fraud, or legal risk contribute significantly to the cost of financial services and where trust is a barrier to uptake of financial services, smart contracts can drive incremental gains in financial inclusion.	7
Smart contracts will not alleviate a variety of common impediments to financial inclusion, including credit risk and income irregularity, distance and inaccessibility, limited awareness and financial literacy, and cultural factors.	7
Among the financial services investigated in this note, smart contracts are more likely to drive financial inclusion gains in supply chain finance and insurance than in consumer credit.	7, Annex
Local financial and legal practitioners with a sound understanding of smart contracts and an intimate knowledge of bottlenecks in financial services contractual processes are likely best positioned to propose tailored smart contract applications relevant for economic development and financial inclusion.	7

Policy Considerations for Responsible and Effective Smart Contract Deployment:	Sections
Local lawmakers and legal authorities will need to determine whether smart contracts are legally binding. Smart contracts can reflect the foundational pillars of contract formation but may not comply with jurisdiction- and transaction-specific contract requirements.	5.1, 6.3
Smart contracts will not prevent fraud, illegality, or unconscionability in the formation process.	5.1, 6.1
Widespread adoption of smart contracts will not eliminate the need for dispute resolution but would give rise to more post-execution cases, in which the ultimate question is whether contract performance should be reversed. Lawmakers and legal authorities will need to evaluate what is optimal or desirable for their own jurisdictions on the burden of proof structure implied in post-execution cases.	5.1, 6.1, 6.3
Legal jurisdictions will need to determine whether computer code is admissible as evidence in court and whether measures need to be taken to convert computer code to natural language.	5.1, 6.3
Policymakers and providers will need to carefully consider how smart contracts will effectively accommodate critical financial consumer protection imperatives, particularly those associated with customer mobility, dispute resolution, unfair and deceptive acts or practices, and disclosure. Disclosure and transparency practices will need to adapt to smart contract characteristics.	6.1
Policymakers and providers will need to ensure that customer due diligence performed in connection with smart contracts meets Financial Action Task Force (FATF) standards, particularly those dealing with Virtual Asset Service Providers and use of third parties to perform customer due diligence.	6.2
Smart contracts that are integrated with digital identifications hosted on a blockchain could ease the implementation of a risk-based approach to customer due diligence. Policymakers should monitor forthcoming FATF guidance on use of digital identifications.	6.2
Standardization and vetting of smart contracts by relevant authorities and stakeholders could minimize risks and increase trust in smart contract applications in retail and MSME finance. Regulators should work with financial services providers to ensure standardized smart contracts meet a variety of minimum criteria prior to deployment.	6.1, 6.4
Policymakers will need to consider whether vetted and other types of smart contracts constitute "general terms and conditions" or another similar legal status, which may entail additional standards related to fairness and clarity.	6.4
Smart contract deployment in a diversity of financial products and services will require extensive connections with external data sources. Governments, standard setting bodies, and international organizations could play a role in facilitating the automation and interoperability of external data sources by identifying types of data widely used in smart contracts, developing standards for ensuring data reliability and transparency, and designing platforms for data dissemination.	6.5

3.

What Are
Smart Contracts

3.1 Origins and Basics

Computer scientist Nick Szabo conceptualized smart contracts in a series of papers in the mid-1990s. He describes smart contracts as, "a set of promises, specified in digital form, including protocols within which the parties perform on these promises." Smart contracts seek to capture contractual elements that are algorithmic in nature and protect agreements from tampering via cryptographic methods.[8]

Many operational elements of contracts essentially represent conditional "if-then-else" statements that are well-positioned for expression in a computer programming language. As an example, consider a weather index insurance (WII) policy that pays a farmer $100 if a rainfall index is below 10 mm in a given month and $0 otherwise. Figure 1 codes the payout agreement that underlies the contract. Recognizing the widespread use of Boolean logic in contracts, smart contract entrepreneurs seek to express such relationships via computer programs.[9]

In addition to their role in expressing aspects of traditional contractual agreements, observers project smart contracts' use in more general code-based agreements. For example, Clack, Bakshi, and Braine's (2017) oft-cited definition of smart contracts advances a flexible conception of the technology: "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

Figure 1. Coding the Underlying Payout Logic in a Weather Index Insurance Policy

```
define payout(rainfall)
        if rainfall < 10:
            payout = 100
            else:
            payout = 0
```

and obligations or via tamper-proof execution of computer code."[10]

Perhaps the two most groundbreaking smart contract properties, for better or worse, are that they are self-executing and immutable.[11] In other words, they execute without human involvement and are unalterable. Smart contract enthusiasts maintain these characteristics will unlock enormous efficiency gains and reduce legal discrepancies. Skeptics tend to be concerned about how smart contracts will handle modification, amendment, or termination due to material change in circumstances or other reasons for full or partial avoidance.

3.2. Smart Contract Typologies

Legal scholars and technology analysts have proposed a variety of typologies that categorize forms of smart contracts based on their purpose, the nature of their legal enforceability, and their interaction with natural language contracts. Table 1 highlights a few of these. One of the most commonly cited typologies distinguishes between "smart contract code" and "smart legal contract."[12] Stark (2016) defines the former as "a specific technology—code that is stored, verified and executed on a blockchain" and the latter, which is an application of the former, as "the use of code to articulate, verify, and enforce an agreement between parties."[13]

Table 1. Select Smart Contract Typologies

"Smart contract code" vs. "Smart legal contract" (Stark 2016)
Smart contract continuum (Chamber 2016: 9): • "Contract entirely in code" • "Contract in code with a separate natural language version" • "'Split' natural language contract with encoded performance" • "Natural language contract with encoded payment mechanism"
"Strong" vs. "weak" (Raskin 2016: 310)
"External" vs. "Internal" (ISDA 2017: 22)
"Integrated" vs. "Non-integrated" (EBRD 2018: 12-13)

Other analysts have proposed similarly useful frameworks. For instance, the Chamber of Digital Commerce describes a rapidly evolving continuum of roughly four smart contract patterns (table 1).[14] One legal scholar proposes a distinction between "weak" and "strong" smart contracts.[15] Legal professionals from the International Swaps and Derivatives Association (ISDA) distinguish between "external" and "internal" smart contracts.[16] The European Bank for Reconstruction and Development (EBRD) draws a distinction between "integrated" and "non-integrated" models of smart contracts.[17]

This note does not take a position on a typology that most effectively describes the current state of smart contracts or add to the list of classifications. Nevertheless, the typologies elucidate the variegated applications analysts envision.

3.3. Blockchain-based Smart Contracts

Until blockchain technology was widely introduced through the development of Bitcoin in 2008, it was not evident what vehicle was best positioned to host smart contracts.[18] In the forward to a 2016 white paper published by the Chamber of Digital Commerce, Szabo argues, "Blockchain technology appears very much to be the jet fuel necessary for smart contracts to become commonplace in business transactions and beyond."[19] Certain blockchain properties, such as its distributed monitoring and consensus mechanism, as well as its cryptographic properties, may forge synergies with smart contracts.[20]

It is this combination of smart contracts and blockchain that offers a new prospect for the digital economy.[21] Various entities conceive of smart contracts as inseparable from blockchain. The U.S. National Institute of Standards and Technology (NIST) defines smart contracts as "a collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network."[22] Similarly, the International Financial Corporation (IFC) describes smart contracts as "self-executing software code that runs on a blockchain."[23]

Consistent with these perspectives, the rest of this note generally contemplates blockchain-based smart contracts. When paired with DLT, particularly blockchain, smart contracts potentially offer a transparent, automated, and efficient way to facilitate various contractual processes, especially monitoring the performance of agreements with less reliance on third parties.

Blockchain-based smart contracts should generally follow a consistent set of phases (figure 2).[24] First, contracting parties agree to and code the terms of their agreement in a smart contract, possibly with the help of a developer. Second, an agreed upon party validates the smart contract and records the agreement on a distributed ledger. Box 1 describes how the nature of this validation process will vary depending on the type of blockchain parties utilize. Third, the smart contract will normally connect with external data sources via database services. These may include a data feed or accounts at financial institutions. Finally, the smart contract will evaluate data and either expire or self-execute based on the terms of the agreement.

Figure 2. Four Basic Stages of a Blockchain-based Smart Contract

Stage 1: Parties strike an agreement and code the terms in a smart contract.

Stage 2: An agreed upon party vaildates the contract and records it to a distributed ledger.

Stage 3: The smart contract connects to relevant external data feeds or systems.

Stage 4: The contract executes or expires based on the terms of the agreement.
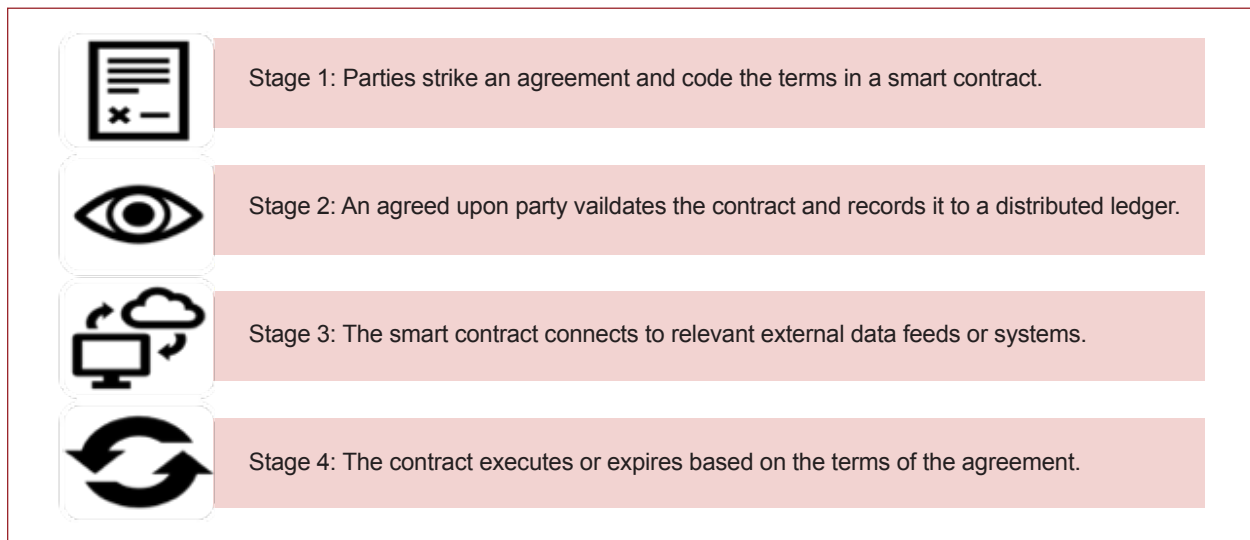
Icon sources: Microsoft Office 365 ProPlus (subscription)

Box 1. Permissionless vs. Permissioned Smart Contract Platforms

The nature of smart contract validation depends on the type of blockchain on which it is hosted. In principle, there are three types of blockchains: public/permissionless, public/permissioned, and private/permissioned. The first dimension refers to the visibility of transactions to the public and participation rules. The second dimension refers to the validation process. On a permissionless platform, smart contracts are validated by anonymous nodes competing for the right to authorize transactions. Ethereum is a well-known example of a permissionless smart contract platform. By contrast, in permissioned systems, participation is regulated by an established vetting procedure and participants are known to one another. The consensus protocols for validating smart contracts in permissioned systems are quite flexible. They could be established by the system's chosen governance body or be transaction-specific. Likewise, parties to a transaction can choose a third-party to validate a smart contract and post it to the blockchain, or they could leverage the resources of a permissioned system designed for enterprise use, examples of which are Hyperledger and Corda.

Sources: World Bank Group (2017). Distributed Ledger Technology (DLT) and Blockchain. Finance, Competitiveness & Innovation Global Practice: Fintech Note No.1.

World Bank Group and Digital Impact Alliance (2018). Technology Landscape for Digital Identification.

4.
Smart Contract Advantages and Efficiencies

4.1. Smart Contracts Seek to Reduce Transaction costs

"The costs that smart contracts address are lumped by economists under the catch-all rubric of 'transaction costs'" (Szabo 1997).

Transaction costs are the search, measurement, bargaining, and enforcement costs inherent in economic exchange. Nobel laureate Douglass North, whose work united transaction costs and institutions with mainstream neoclassical economic analysis, developed a prominent working definition of transaction costs, explaining, "The costliness of information is key to costs of transacting, which consist of the costs of measuring the valuable attributes of what is being exchanged and the costs of protecting rights and policing and enforcing agreements."[25] Smart contracts attempt to minimize reliance on existing institutions, such as third-party enforcement mechanisms and financial institutions, which facilitate economic exchange.[26]

Among the different types of transaction costs, smart contracts most clearly address enforcement costs. Enforcement costs, broadly defined, consist of the cost of maintaining and using third-party enforcement mechanisms, as well as ongoing monitoring and verification of economic agreements. Smart contracts seek to directly reduce enforcement costs in three ways. First, they increase the cost of breach through self-execution and immutability, thereby reducing uncertainty, the likelihood of contract defection, and, ultimately, the need to maintain and use costly third-party enforcement mechanisms (figure 3).[27] Second, smart contracts' use of automated control protocols reduce the cost and increase the speed and accuracy of monitoring and verification.[28] Finally, smart contracts' use of blockchain establishes transparent monitoring that is accessible to all parties, without the need for costly replication. On a more macro-level, economists argue these properties will increase the universe of feasible contracts.[29]

Smart contracts' role in reducing other forms of transaction costs is less straightforward. Search and measurement costs refer to costs associated with the pursuit of transaction opportunities and the valuation of the assets underlying exchange. Smart contracts do not reduce these costs directly. However, to the extent that smart contracts facilitate greater automation in and enhance the efficiency of key players involved in the search and measurement process, such as financial institutions and lawyers, they may indirectly help reduce search and measurement costs. To benefit end-users, institutions

Figure 3. Contract Performance as a Function of the Cost of Breach

4.2. Specific Gains for Firms and Consumers

Smart contracts may unlock value for firms and consumers through automation, self-execution, immutability, and distributed access and verification. Table 2 summarizes the sources of some potential benefits from the use of blockchain-based smart contracts for financial institutions and their customers.

Financial institutions may experience a variety of efficiency gains ranging from reduced operating costs, better risk management, and enhanced coordination, among others. Enhanced automation should help financial institutions reduce operating costs, operational risk, and physical documentation. Self-execution and immutability would reduce operational risk and counterparty risk. Distributed access and verification will influence most of cited factors. Meanwhile, customers stand to gain in terms of reduced service cost, potential increase in product and service access, and improved timeliness and transparency, among

experiencing efficiency gains from automation would need to share the gains with their customers. Smart contracts may also reduce bargaining and settlement costs to the extent that they foster more transparency and confidence in contract performance.

Table 2. How Could Smart Contracts Unlock Value in Financial Services?

Anticipated Effects of Smart Contracts		Primary Source of Benefit		
		Automation	Self-execution & immutability	Distributed access & verification
Financial institutions — Operating cost (overhead, service)	↓	✓	✓	
Legal and auditing fees	↓	✓	✓	✓
Operational risk	↓	✓	✓	✓
Counterparty risk	↓		✓	✓
Data concentration risk	↓			✓
Records replication	↓			✓
Physical documentation	↓	✓		✓
Coordination ease	↑			✓
Verification ease	↑			✓
Customers — **Service cost**	↓	✓		✓
Trust barrier	↓		✓	✓
Uncertainty	↓		✓	✓
Access	↑	✓		✓
Timeliness	↑	✓	✓	✓
Transparency	↑			✓

other areas. Importantly, some key customer benefits, particularly lower service cost and enhanced access, will depend on financial institutions sharing the benefits of efficiency gains with consumers.

4.3. Smart Contracts and Peer-to-Peer Transactions

This note generally focuses on financial intermediaries' use of blockchain-based smart contracts. However, an ideal transaction for smart contract purists eliminates third-party involvement altogether. Purists envision smart contracts facilitating self-enforcing peer-to-peer (P2P) economic interactions, with little involvement from financial intermediaries, lawyers and courts.[30] To the extent that smart contracts and blockchain facilitate more P2P transactions with reduced reliance on third-parties, the relative weight of measurement

and enforcement costs will shift. In smart-contract-facilitated P2P transactions, direct costs associated with third-parties, such as financial intermediaries and enforcement mechanisms, would disappear.

Indirect measurement costs would not disappear on account of smart contracts and blockchain alone. Searching for transactions, valuing the underlying assets, and bargaining are difficult and time-consuming tasks. One of the values of financial intermediaries who specialize in measurement is to reduce such costs by freeing up economic actors to focus on more productive activities. However, some observers project that the confluence of smart contracts, blockchain, AI, and the Internet of Things (IoT) may facilitate dis-intermediation to the extent that these technologies can link potential counterparties directly. [31]

5.
Legal Aspects of Smart Contracts

5.1. Smart Contracts and Contract Law

The use of computer code to establish an agreement on mutual obligations should not, in and of itself, negate smart contracts' legality and enforceability. A contract is "an agreement between private parties creating mutual obligations and enforceable by law."[32] The core tenets of a contract do not depend on a specific type of capturing mechanism. Contract formation occurs in Civil Law jurisdictions when offer meets acceptance. In Common Law jurisdictions, and for certain types of contracts in Civil Law jurisdictions, contract formation occurs when offer and acceptance are based on consideration. Smart contracts can meet these foundational contract elements, which reflect the human interactions that underpin a contractual agreement. Smart contracts may not meet jurisdiction- and transaction-specific enforceability requirements (figure 4).

Figure 4. Smart Contracts and the Elements of Contract Enforceability

Foundational Contract Information Pillars			Smart contract suitability
Offer	Acceptance	Consideration	✔
Jurisdiction- and Transaction-specific Requirements			Smart contract suitability
Form	Interpretation		⚠
	? `define contract(x)` `if x:` `pay = 0` `else:` `pay = 0`		

Icon sources: Microsoft Office 365 ProPlus (subscription)

In many cases, jurisdictions require contracts to take on a specific type of form, such as written form, either in general or for certain classes of transactions. Whether smart contracts qualify as written form will be locally determined. Moreover, jurisdictions have differing standards for contract interpretation and understanding. Problematically, common high-level programming languages do not represent the actual code a computer reads, which may raise interpretation issues in a court of law.[33] Jurisdictions may also require signatures from authorized persons or notaries. Thus, notwithstanding their ability to reflect the foundational elements of contract formation, whether judiciary systems are prepared for or willing to admit smart contracts in court is a complex matter and will vary across jurisdictions.

Smart contracts will shift certain points of emphasis in contract law practices. A brief distinction between smart contracts and common digitally-enabled contracts may be useful. Today, a contract might be programmed into a system and could take certain actions, such as crediting or debiting an account. The laws pertaining to digital signatures allow for consent to be issued electronically. However, the integrity of what is signed and executed is controlled by a particular institution, such as a bank.

Smart contracts seek to eliminate (in permissionless systems) or limit and bring greater transparency to (in permissioned systems) intermediaries' control over this process. Moreover, smart contracts seek to shift the balance in contractual relationships toward performance over breach and proactive over retroactive enforcement.[34] Assuming the outcome of a contract is a payment, a smart contract should self-execute when the conditions of the contract have been met, provided that the payer in a contract has adequate funds and the smart contract is linked to the payer's bank account.

One area legal professionals project issues is in the realm of modification. Due to smart contracts' immutability, they may not adapt well to changing circumstances.[35] Amending would still require active involvement of both parties. One potential approach to modification is to engage in the simultaneous annulment of an existing smart contract and the formation of a new one, but the consequences of such an approach would need to be evaluated on a case-by-case.

Smart contracts will not prevent fraud, illegality, or unconscionability in the formation process. As a corollary, smart contracts will not eliminate the need for dispute resolution and third-party legal intervention. To echo a recent analysis of blockchain's potential for economic development, the combination of smart contracts and blockchain represents a "garbage-in-garbage-out" system.[36] The technology itself cannot solve human-driven abusive practices in the contract formation phase. On the contrary, smart contracts might facilitate such practices because they are immutable and execute once contractual parameters are met, irrespective of the nature of those parameters. As the CFTC aptly states, if a "smart contract violated the law, it would not be binding or enforceable."[37] Thus, courts will still need to address these matters and evaluate defenses to formation.[38]

If smart contracts are widely adopted, courts will likely hear more post-execution, rather than pre-execution cases.[39] Smart contracts may also expand instances of defense to formation based on the understandability of terms, particularly in retail finance, as computer code literacy is not widespread in the general public.[40] To enable effective dispute resolution, developers and lawyers may be able to create programs that would allow parties to freeze the execution of smart contracts linked to arbitration and dispute resolution clauses. However, a question arises as to whether the possibility of freezing execution takes away the defining characteristics of a smart contract – self-execution and immutability.

5.2. Smart Contracts' Likely Contractual Role

Smart contracts will most likely complement, but not displace natural language contracts in the near-term. Rapidly evolving technological capability can radically alter existing institutional arrangements. It is therefore difficult to predict smart contracts' future scope of use for contractual purposes. Nevertheless, in the near-term, many legal analysts project smart contracts could probably play some variation of two roles in contractual agreements.[41] First, they may simply serve as a payment mechanism associated with a fully natural language contract. Second, they could capture certain

operational contract elements that are expressible in straightforward conditional logic. For example, smart contracts could represent unambiguous, conditional if-then statements embedded in many contracts. Therefore, actual contract elements would be written in code. Other aspects would remain in natural language, particularly non-operational elements and those that require judgement, subjective analysis, and the use of complex legal principles (e.g., "reasonableness," "good faith").

Smart contracts will struggle to capture circumstances that call for fallback clauses. Some argue that because ambiguity does considerable violence to computer programs, smart contracts will productively force contractual parties to eliminate ambiguity and contemplate all possible contingencies ex-ante. Though it is certainly useful to carefully evaluate the range of possible future scenarios, there is a cost-benefit dynamic to such an exercise.[42] Indeed, catch-all or fallback clauses are often embedded in contracts because it is difficult to foresee all future circumstances. Attempting to do so ex-ante may pose extraordinary challenges to concluding transactions in a timely manner. Ironically, ambiguity can in some cases enhance efficiency by allowing parties to contract now and dispute later if something goes wrong.

6.
Policy Considerations for Responsible and Effective Smart Contract Deployment

Sections 6.1-6.5 discuss a series of policy considerations that local authorities, standard setting bodies, and international organizations should evaluate to ensure smart contracts' responsible and effective deployment. Section 6 focuses on financial consumer protection, customer due diligence, foundational legal determinations, standardization and vetting, and data source automation. This is not an exhaustive list of policy considerations related to smart contracts. Other considerations include governance, privacy, cyber security, and many others. Future research should address these other areas. The World Bank will continue to vet possible enabling measures and policy guidance for smart contracts.

6.1. Financial Consumer Protection

Smart contracts' suitability for and uptake in retail finance will depend heavily on their compatibility with good financial consumer protection (FCP) practices. Protecting consumers from abusive financial practices has become a central goal of financial public policymakers worldwide. The Global Financial Crisis revealed that the quality of a jurisdiction's consumer protection practices has direct implications for financial stability and economic health. FCP is a critical consideration for innovative financial services channels. The WBG's 2017 Good Practices for Financial Consumer Protection (GPs) serve as a comprehensive reference and toolkit for FCP policy approaches. Though not exhaustive, this section highlights aspects of the GPs that will be vitally important and, in some cases, challenging within the context of smart contracts' use in retail finance.

Importantly, innovation and FCP are far from incompatible. The GPs urge policymakers to consider flexible regulatory arrangements that can accommodate "innovation in product design and delivery."[43] In fact, if regulators have access to blockchains on which smart contracts are hosted, such technology could facilitate FCP oversight in retail finance. Nevertheless, policymakers and practitioners will need to carefully consider how the deployment of smart contracts in retail finance accommodates a variety of FCP imperatives, particularly allowing customer mobility, providing for dispute resolution, preventing unfair and deceptive acts or practices, and disclosure.

Customer mobility and dispute resolution pose the most significant FCP challenges for smart contracts. The GPs stipulate a variety of customer mobility standards, including prohibiting "unduly limiting a customer's ability to cancel or transfer a product or service to another service provider" and providing customers a cooling-off period in many cases.[44] The GPs further outline the need for robust complaints handling and dispute resolution mechanisms.[45] The nature of customer mobility and dispute resolution within the context of smart contracts is unclear. In their purest form, smart contracts do not contemplate the need for such mechanisms. However, providing for customer mobility will remain a vital condition for consumer financial products. Furthermore, smart contracts will not eliminate the need for dispute resolution. Therefore, providers and policymakers should ensure smart contract-facilitated retail finance products incorporate appropriate customer mobility requirements and offer robust complaints handling and dispute resolution options.

A variety of smart contract characteristics that supporters cite as clear advantages, such as self-execution and immutability, are more likely context-dependent for FCP purposes. As discussed in section 5.1, smart contracts' immutability and self-execution are not advantageous properties when the terms they capture are illegal, fraudulent, or unconscionable. Rather, in these cases, smart contracts exacerbate abusive contractual arrangements by narrowing the window for dispute and recourse. Thus, the GPs related to unfair terms and conditions, unfair practices, and sales practices are crucial for smart contracts.[46] The GPs state that financial agreements based on unfair terms and conditions "should be void and legally unenforceable."[47] The self-executing and immutable nature of smart contracts must not undermine this necessity.

Providers and policymakers will need to adapt disclosure and transparency practices and standards to smart contract characteristics. On the whole, deploying a financial product or service via smart contracts will not change a financial service provider's disclosure and transparency obligations with respect to that product. Moreover, the potentially enhanced contract transparency afforded by smart contracts could propel financial institutions to raise the quality of their disclosure practices. Still, providers and policymakers will clearly need to consider certain disclosure issues for smart contracts. For instance, the GPs stipulate that providers must furnish disclosure in plain, easy to comprehend, and local language that is understandable by an average person. In this light, it will be important to use the disclosure process, particularly key facts statements, to clearly address any confusing aspects surrounding the use of the smart contract in the agreement. Additionally, the GPs lay out guidelines for disclosing the right to termination and material changes in terms. As illustrated in the Annex, such disclosure may be difficult to incorporate in smart contracts, though this owes more to the nature of the smart contract, rather than a challenge with disclosure itself.

Some of the FCP imperatives and risks associated with smart contracts could be addressed through vetting and standardization pursued by regulators and other stakeholders (see: section 6.4). Many consumer financial contracts are already quite standardized and must conform to specific FCP standards. Regulators could similarly work with financial services providers to develop vetting procedures that ensure standardized smart contracts meet certain minimum FCP criteria prior to deployment. Moreover, ongoing developments in regulatory and supervisory technology that leverage machine learning and AI could facilitate solving some of the disclosure challenges highlighted above.

6.2. Customer Due Diligence

Many countries maintain laws and regulations related to customer due diligence (CDD) as part of anti-money laundering (AML) and combatting the financing of terrorism (CFT) frameworks. Countries often look to the Financial Action Task Force (FATF)'s recommendations for guidance on designing CDD standards. Blockchain-based smart contracts present challenges and opportunities for CDD. Key issues involve the nature of anonymity on a blockchain, digital identities, and use of third parties to perform CDD.

The FATF's baseline recommendations for the CDD aspects of AML/CFT standards require financial institutions to identify and verify customer identities, identify beneficial owners, ascertain the purpose

of a customer's business, and conduct ongoing monitoring.[49] To balance the twin imperatives of financial integrity and financial inclusion, the FATF recommends that countries adopt a proportional, risk-based approach (RBA) to CDD. Examples of an RBA include exemptions for proven low risk customers, simplified due diligence (SDD) for evidence of low risk, and accepting alternative, including digital, forms of identification.[50]

The type of blockchain on which smart contracts are hosted (see: Box 1) could introduce complexity for AML/CFT compliance. Anonymity of parties to a smart contract, which is especially characteristic of public, permissionless blockchains, are difficult to square with basic CDD requirements and standards related to reporting suspicious transactions to authorities. Smart contracts hosted on permissioned blockchains are, in this sense, more easily amenable to AML/CFT compliance.

The FATF has taken a number of steps to ensure that Virtual Asset Service Providers (VASPs) adhere to the same CDD standards as other financial institutions. VASPs include those entities that provide virtual assets necessary for executing smart contracts on public, permissionless blockchains. As countries consider CDD standards within the context of smart contracts, they should consult relevant FATF resources. These include FATF Recommendation 15 on New Technologies, the Interpretive Note to Recommendation 15, and the definitions of virtual assets and VASPs, all contained in the FATF's International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.[51] Additionally, countries should consult the FATF's Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.[52]

Smart contracts that are integrated with digital identifications hosted on a blockchain could ease the implementation of an RBA to CDD. The FATF observes that digital identifications can "improve the reliability, security, privacy, convenience and efficiency of identifying individuals in the financial sector, to the benefit of both customers and regulated entities."[53] To this end, FATF is in the process of developing guidance that will help governments and financial institutions apply the RBA when digital identifications are employed, having released a consultative document on the topic in November 2019.[54] The draft guidance focuses on helping users evaluate the reliability and independence of digital identities and whether these properties are commensurate with the illicit finance risks posed within a given country.

FATF Recommendation 17 permits countries to allow financial institutions to rely on third parties to perform CDD, provided certain criteria are met. Among other criteria, the third party itself must be supervised for and compliant with the country's CDD standards, and the financial institution needs ready access to all the key elements of CDD performed by the third party. Ultimate responsibility for ensuring appropriate CDD lies with the financial institution.

Third party CDD has relevance for smart contracts because nearly all current smart contract use cases envision leveraging a blockchain platform managed by a third party. Use cases also project consortia of financial institutions interacting on a blockchain platform. Not all countries allow third parties to perform CDD. In countries where use of third parties for CDD is permitted, authorities will need to evaluate how CDD responsibilities are delineated in blockchain-based smart contracts and whether CDD that is being performed through the blockchain is compatible with FATF Recommendation 17.

6.3. Foundational Legal Determinations

Section 5 discusses the key legal aspects of smart contracts. This section builds on section 5 by highlighting select legal determinations local authorities will need to make as they consider how smart contracts will fit in their own legal systems. The section draws on the EBRD's report entitled, "Smart Contracts: Legal Framework and Proposed Guidelines for Lawmakers," which contains extensive analysis of legal considerations within the context of smart contracts, including: "existence and fundamental elements of valid and binding contracts," "challenges to the validity and binding nature of smart contracts," "addressing deficiencies and mistakes in smart contracts," "amendments to smart contracts," "governing law and jurisdiction," "dispute resolution," and other topics.[55]

The first determination authorities need to make is whether smart contracts are able to represent legally binding contracts. As argued in section 5.1, smart contracts can meet the foundational pillars of a contract—offer, acceptance, and, in common law jurisdictions, consideration. Therefore, the key considerations will revolve around whether smart contracts meet jurisdiction-specific legal formalities. Additionally, given that smart contracts are anticipated to assume many duties previously executed by contract parties, jurisdictions will need to determine whether a smart contract has "legal capacity" or, more realistically, whether a smart contract is acting as a communication mechanism. If the latter, the EBRD argues that jurisdictions will need to further determine whether "conditional" offer and acceptance are valid for a legally binding contract.

In section 6.4, this note proposes that certain smart contracts would benefit from external vetting and standardization, particularly in the retail and MSME finance context. Jurisdictions will need to consider whether vetted and other types of smart contracts constitute "general terms and conditions" or another similar legal status. Often, general terms and conditions must meet certain fairness and clarity

standards, which is likely beneficial for retail and MSME finance.

As argued elsewhere, smart contracts will not eliminate the need for dispute resolution, but there are a variety of considerations countries should evaluate with respect to smart contract-related dispute resolution. Perhaps most importantly, if smart contracts are widely adopted, courts will likely hear more post-execution cases, in which the ultimate question is whether contract performance should be reversed. The EBRD points out that post-execution cases shift the typical burden of proof considerably. The claimant in post-execution cases, for which the contract outcome is a payment, will often be the payer, and the payer will need to demonstrate that contract performance should be reversed (figure 5).

The shift in burden of proof for post-execution cases would have major implications in the financial inclusion context, particularly for situations in which consumers and MSMEs are payers, as is the case for loan payments and insurance premiums. On the one hand, the shift may make financial institutions more willing to provide certain financial services. On the other hand, it could place significant legal risk on

Figure 5. Typical Claims: Pre-execution vs. Post-execution Cases
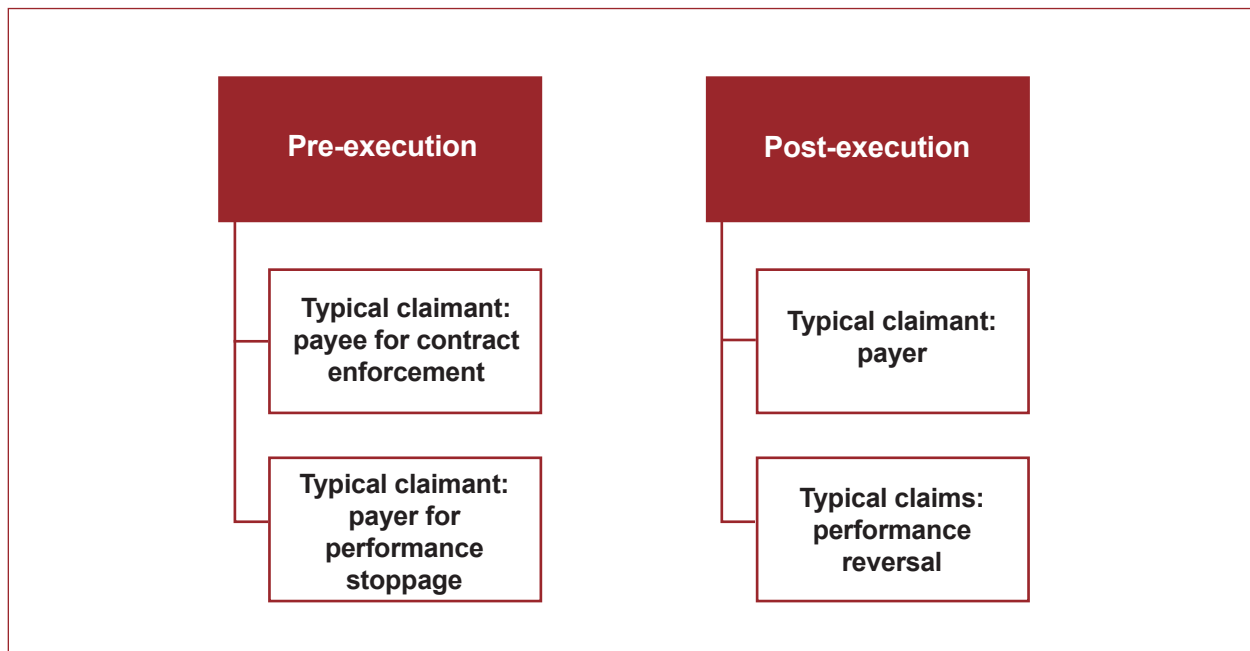
consumers and MSMEs, who are resource-poor compared to financial institutions.

Policymakers will need to evaluate what is optimal or desirable for their own jurisdictions on the burden of proof structure implied in post-execution cases. They can take indirect measures to ensure consumers and MSMEs do not assume excessive legal burden, such as ensuring strong FCP standards (see: section 6.1) and pursuing standardization and vetting for smart contracts (see: section 6.4). More directly, policymakers could identify certain settings, such as retail and MSME finance, where the burden of proof structure in post-execution cases is unacceptable and take measures to alter relevant legal standards.

Legal authorities will need to evaluate a variety of other issues that will arise in disputes. For example, legal jurisdictions will need to determine whether computer code is admissible as evidence in court and whether measures need to be taken to convert code to natural language. Legal authorities will also need to determine whether arbitration is acceptable for smart contracts. Moreover, courts will need to consider how the allocation of liability will unfold in the case of smart contract mistakes and deficiencies. Many of these considerations will likely play out on a case-by-case basis.

6.4. Standardization and Vetting

Standardization and vetting of smart contracts by relevant authorities and stakeholders could minimize risks and increase trust in smart contract applications in retail and MSME finance. Financial and technology regulators, financial institutions, and smart contract developers should work together to ensure smart contract financial products meet FCP standards and do not present significant operational risk, such as coding errors that could substantially alter or invalidate contract terms. Participating stakeholders could also develop plain language disclosures associated with vetted smart contracts. Additionally, smart contracts could incorporate checks to ensure compliance with certain standards, including, for instance, age requirements for financial products, right over assets, and validity of consent.

Standardization and vetting would provide a minimum level of trust and transparency to retail and MSMEs customers, who might not have the resources or sophistication to thoroughly evaluate smart contract transactions. Vetted smart contracts would likely be considered "general terms and conditions," or have a similar designation in many legal jurisdictions, for which additional standards related to fairness and clarity apply.[56] Moreover, a common understanding of certain smart contracts terms could enable legal and regulatory professionals to easily scrutinize the contracts, if necessary.

6.5. Data Source Automation

Smart contracts often require connections with external data sources relevant for contract terms. Examples include macroeconomic data, environmental indicators, credit reporting information, global positioning, public registries, and many others. Smart contract deployment in a diversity of financial products and services will require extensive connections with such data sources. Governments, standard setting bodies, and international organizations could play a role in facilitating the automation and interoperability of data sources necessary for smart contract applications. Task forces established by such bodies could focus on identifying types of data widely used in smart contracts, developing standards for ensuring data reliability and transparency, and designing platforms for data dissemination.

A related task involves pursuing the machine readability of law and legal documents. As discussed in section 5 and in the Annex, smart contracts are currently best positioned to incorporate straightforward, operational elements of contracts. However, advancements in natural language processing (NLP) could help expand the range of content smart contracts could evaluate. If blockchain and smart contracts are widely adopted, it may be productive for governments and the private sector to allocate resources to NLP projects that advance the machine readability of law and legal documents.

7.
Potential Smart Contract Applications and Financial Inclusion Implications

Observers have speculated about smart contracts' use in a variety of financial services. Sections 8.1 - 8.3 discuss potential smart contract applications in supply chain finance (SCF), insurance, and consumer credit, three commonly cited smart contract use cases with implications for financial inclusion. The sections focus on how smart contracts would change the provision of these financial services and the incremental gains in financial inclusion smart contracts could engender.

Barriers to financial inclusion are variegated. Some common hurdles to financial inclusion include: cost of financial services, trust in financial institutions, identification and documentation, distance and accessibility, awareness and financial literacy, income regularity and creditworthiness, and other cultural and religious factors. Among these, smart contracts have clearest relevance for cost and trust.[57] Thus, incremental financial inclusion gains will depend on their ability to reduce the cost of providing financial services and help overcome the trust barrier.

7.1. Supply Chain Finance

The WBG and IFC estimate the finance gap among formal and informal MSMEs to be 18 percent and 11 percent of developing economies' GDP, respectively.[58] The MSME finance gap varies considerably across regions (figure 6). Access to finance for working capital purposes, which is the focus of SCF, is a key element of the finance gap among MSMEs. Smart contracts hold promise for reducing process frictions and improving information asymmetries that constrain SCF for MSMEs. Though smart contracts can play a role in enabling access to SCF for MSMEs as buyers, such as when small merchants make inventory purchases from suppliers, this section focuses on smart contracts' role in facilitating SCF for MSMEs as suppliers of larger customers. Use case thinking is more developed in this latter scenario.

When MSMEs sell products to commercial and government buyers, they typically offer terms that allow delayed payment. The MSME prefers that the buyer pays quickly, but the buyer prefers to delay payment as long as possible. Financial institutions can step in to partially resolve this clash of preferences. A common service that financial institutions offer for alleviating the working capital pressure associated with cash conversion cycles is invoice discounting.

Figure 6. The MSME Finance Gap Across Developing Regions (Percent of GDP)
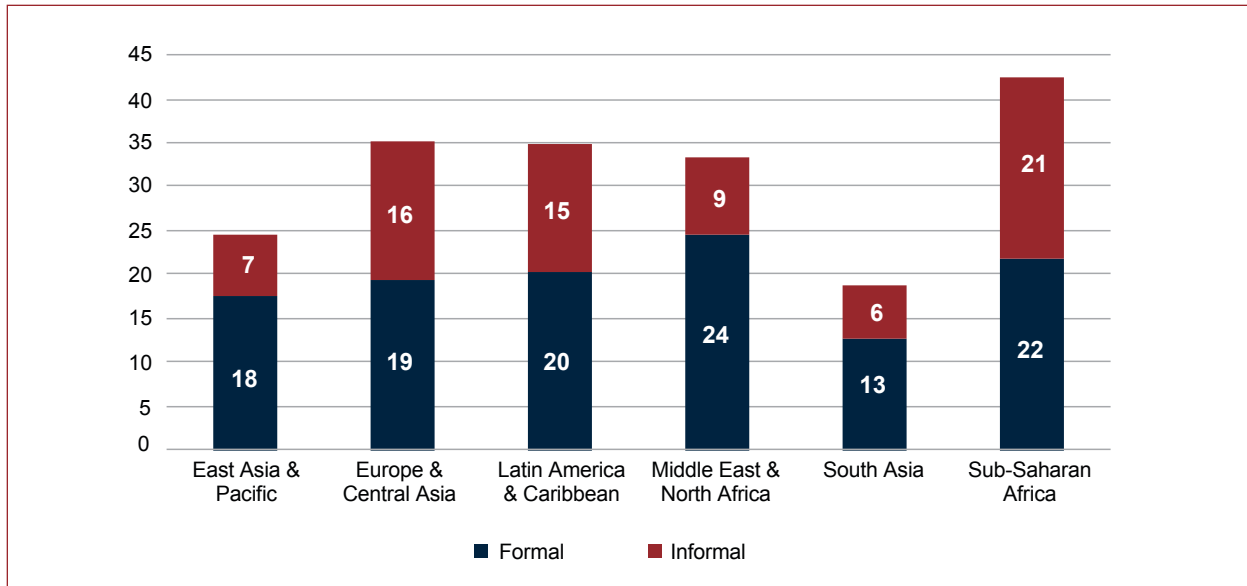
Source: IFC, MSME Finance Gap Database, October 2018 Update.

A typical invoice-discounting transaction involves a few phases. When an MSME sells goods to a buyer, it simultaneously invoices the buyer. Assuming the goods are properly delivered, the buyer approves the invoice and registers it with the financial institution, often via an SCF platform. Once the invoice is recognized as collateral by the financial institution, the MSME can request a discounted amount of the invoice from the financial institution. Finally, when the buyer pays off the invoice to the financial institution, the transaction is settled.

An advantage of invoice discounting over other working capital finance models is that financial institutions evaluate the creditworthiness of the buyer, which is typically larger and more sophisticated than the supplier and, in some cases, is already a customer of the financial institution. The creditworthiness of the MSME is not the primary driver of access to invoice discounting. Therefore, to the extent that smart contracts can alleviate process frictions and improve transparency, they could facilitate meaningful improvements in access to invoice discounting for MSMEs.

Smart contracts could help simplify the complex multiparty system that underlies SCF by reducing informational asymmetries, increasing speed and efficiency, and, ultimately, driving down cost. Invoice discounting smart contracts would likely be hosted on a permissioned blockchain administered by a financial institution or a third party SCF platform. Figure 7 summarizes how smart contracts could drive process improvements, fraud reduction, and enhanced transparency in invoice discounting, all of which could facilitate the provision of invoice discounting.

Importantly, advancements in IoT would complement the properties highlighted in figure 7 by enabling transparent, real time tracking of items flowing through the supply chain. In this sense, smart contracts and IoT would facilitate better supply chain management by enforcing conditional workflow, which would ease the provision of SCF.

Figure 8 tracks the flow of items in an SCF transaction. All three parties to the transaction would gain individual-specific process improvements and common benefits from the use of blockchain, smart contracts and IoT. Invoicing and title transfer could be automated for MSMEs. Buyers could use automated receipt-of-goods verification, invoice approval, and invoice transfer to the financial institution. The financial institution could automate the release of discounted funds to the MSME.

Figure 7. How Could Blockchain-Based Smart Contracts Expand Access to SCF?

Process improvements	• Facilitation of automated invoicing, verification, and approval • Improved risk estimation and speed of invoice approval through supply chain items' immutable record of activities
Fraud reduction	• Reduced fraud risk through unique, immutable invoices and record of supply chain items' activities
Enhanced transparency	• Transparent storage of credit ratings, supplier evaluations, and reputational information • Transparent title transfer

Sources: Yaksick, Rudy (2019), Overcoming Supply Chain Finance Challenges via Blockchain Technology. In Disruptive Innovation in Business and Finance in the Digital World. International Finance Review, Volume 20, 87-100. Emerald Publishing Limited; Templar, Simon, Erik Hofmann, and Charles Findlay (2016), Financing the End-to-End Supply Chain: A Reference Guide to Supply Chain Finance, Kogan Page Limited.

Figure 8. The Flow of Items in a Supply-Chain Finance Transaction Facilitated by Blockchain, Smart Contracts, and the Internet of Things
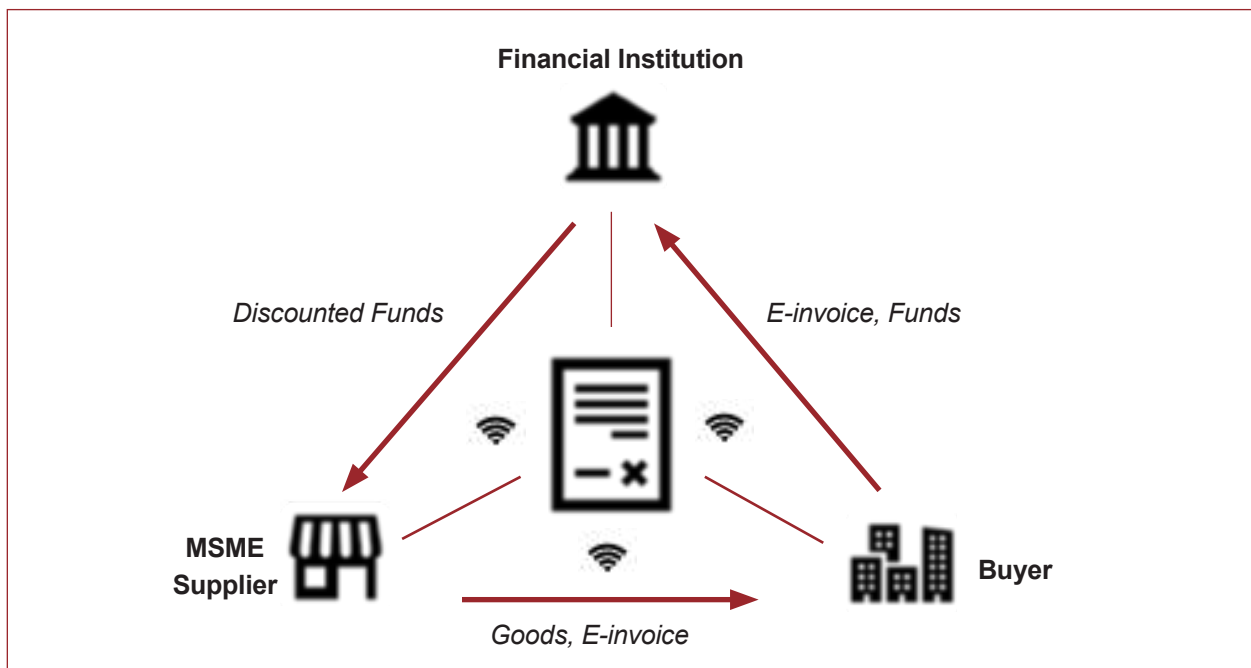
Icon sources: Microsoft Office 365 ProPlus (subscription)

All parties would gain increased visibility of item flow and more transparent reputational information. This is particularly important for the financing company, whose willingness and ability to provide SCF is linked to visibility of items flowing through the supply chain. Box 2 profiles a blockchain developer, Sofocle, which is leveraging these technologies to offer SCF solutions.

7.2. Insurance

Certain types of insurance policies present opportunities for relatively straightforward smart contract applications. Index-linked insurance, such as WII, and other forms of disaster insurance may be particularly well-suited for smart contracts to the extent that underlying events (e.g., rainfall index) can be deterministically coded. Figure 9 depicts the coming together of smart contracts and blockchain within the context of the example WII policy introduced in section 3.1.
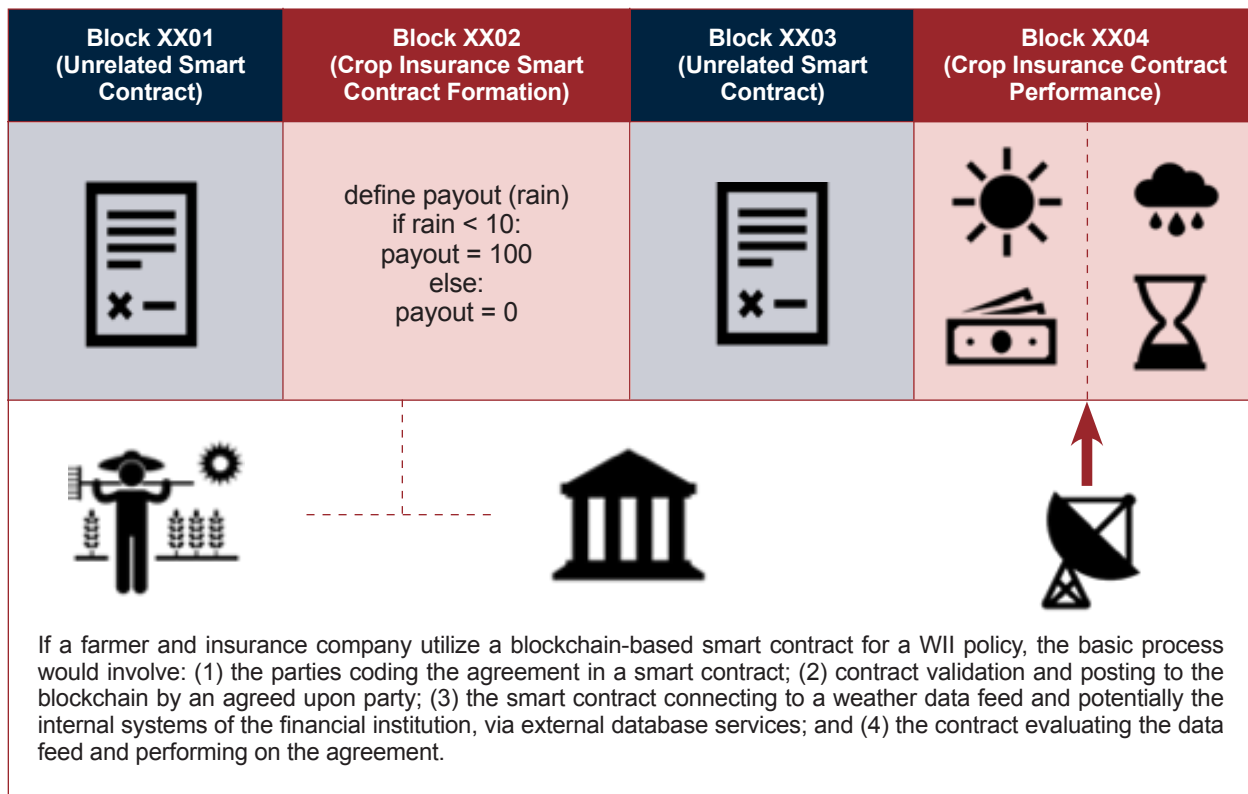
Box 2. Sofocle Technologies

Sofocle Technologies, a blockchain solutions provider based in India, integrates blockchain, smart contracts, and IoT in its SCF solution, sofoCap, and its supply chain management solution, Certum. Both solutions use the concept of "tokenization" to make key aspects of the supply chain fit for exchange in a virtual environment. With sofoCap, tokenization involves making e-invoices unique and immutable, in order to reduce double invoicing and fraud. Similarly, Certum creates a "digital passport" for physical objects, so they can be tracked and traced throughout the supply chain, thereby increasing visibility and reducing counterfeiting risk. According to Sofocle, sofoCap can be used to automate invoice reconciliation, disbursal, and repayment, among other tasks. Sofocle uses the HyperLedger blockchain platform.

Sources: Sofocle, sofoCap: https://www.sofocle.com/solutions/blockchain-in-supply-chain-finance-sofocap/

Sofocle, Certum: https://www.sofocle.com/solutions/blockchain-in-supply-chain-management-certum/

Figure 9. The Basic Structure of a Weather Index Insurance Smart Contract

Block XX01 (Unrelated Smart Contract)	Block XX02 (Crop Insurance Smart Contract Formation)	Block XX03 (Unrelated Smart Contract)	Block XX04 (Crop Insurance Contract Performance)
	define payout (rain) if rain < 10: payout = 100 else: payout = 0		

If a farmer and insurance company utilize a blockchain-based smart contract for a WII policy, the basic process would involve: (1) the parties coding the agreement in a smart contract; (2) contract validation and posting to the blockchain by an agreed upon party; (3) the smart contract connecting to a weather data feed and potentially the internal systems of the financial institution, via external database services; and (4) the contract evaluating the data feed and performing on the agreement.

Icon sources: Microsoft Office 365 ProPlus (subscription), except "Farmer," Gan Khoon Lay, Noun Project.

After the farmer and the insurance company have the terms of a WII policy coded in a smart contract, a chosen party would validate the smart contract and post it to the blockchain. The blockchain, in turn, connects to an agreed upon weather data feed via an "oracle", a third-party service that exists for the sole purpose of connecting blockchains to external sources. The blockchain may also interact with the internal system of the financial institution to verify premiums and extract payouts. Depending on value of the rainfall index, the smart contract executes or expires.

The Annex draws excerpts from the terms and conditions of a WII policy and analyzes how smart contracts would change key elements of the policy. Certain operational elements based on conditional logic, which form the backbone of the agreement, are well-suited for smart contracts. However, non-operational elements and those involving discretion or judgement may still require separate natural language documentation. Smart contract use will fundamentally alter other elements, such as those addressing the claims process and dispute resolution. If, for instance, WII smart contract policies are designed under the presumption of normal rainfall and only execute upon deviations from normal rainfall, clauses protecting against customer misrepresentations will be unnecessary.

WBG FinTech Note No. 2, which explores how innovative technologies can make insurance more inclusive, outlines the impediments to insurance penetration among individuals worldwide.[59] These include low incomes, constrained understanding and awareness, unsuitable products, distribution, and business models, and limited trust. Smart contract adoption in the insurance space will not improve income and awareness, but it could potentially address suitability and trust.

To the extent that smart contracts help lower the cost of providing insurance, insurers could focus more resources on product, distribution, and business model suitability. WBG FinTech Note No. 2 explains that the insurance industry is still dominated by manual, paper-based processes that are susceptible to glitches. Smart contracts could be effective in alleviating frictions in the claims process, including those involving paperwork filing, handling, investigation, and settlement. Smart contracts could also streamline premiums collection

and other administrative tasks, thereby improving insurance company efficiency.

Regarding trust, smart contracts would help improve transparency and move at least some of the control over the claims process out of the hands of the insurance company. This could instill greater trust in the process. Additionally, in some deterministic cases, smart contracts may enable fully automated claims, eliminating the burden on customers to file claims, thereby improving timeliness and reducing the uncertainty of payouts. Improvements in the timeliness and certainty of claims payments could enhance trust in insurance companies and demand for insurance products.

Initially, smart contract insurance deployments will likely focus on higher-level, less consumer-facing products, such as reinsurance. Box 3 profiles one such deployment—the insurance consortium B3i's property catastrophe reinsurance smart contract prototype.

7.3. Consumer Credit

Smart contract applications in consumer credit are less straightforward and less likely to drive incremental financial inclusion gains than smart contract applications in SCF and insurance. A significant driver of the cost of consumer credit is the credit risk of the borrower. Smart contracts will do little to improve borrowers' creditworthiness. Therefore, smart contracts' ability to meaningfully reduce the cost of providing consumer credit, particularly short-term unsecured loans, may be limited.

Still, smart contracts could yield efficiency gains across various phases of a loan's lifecycle. Many forms of consumer credit involve intense, step-by-step processes that entail significant fees and third-party involvement. Even in advanced economies, some consumer credit processes, such as home and auto lending, still depend on paper-based work streams. As with SCF and insurance, smart contracts could help automate certain aspects of consumer lending. It is worth noting, though, that the application and approval processes for many forms of unsecured lending, such as credit cards and mobile money-based loans, are already highly automated.

A commonly cited smart contract use case is for mortgage loans. The mortgage loan work-flow typically involves a set of lengthy, conditional steps that depend on human-centric approvals. Analysts maintain smart contracts could be integrated into the entire loan process, including pre-contractual phases, such as application processing and underwriting, by enforcing the conditional work flow, reducing paperwork, and connecting more easily to necessary external data (e.g., credit bureaus).[60] When loans enter servicing, smart contracts could fulfill many loan servicing tasks, such as collecting and disbursing payments to loan holders, tax authorities, and insurance companies (figure 10).

The Annex examines excerpts from the terms and conditions of a mobile money-based, short-term unsecured loan, a type of financial product often analyzed within the context of financial inclusion. As with the WII policy, smart contracts could effectively code loan terms reflecting straightforward conditional logic. However, non-operational elements and those that entail judgement, discretion, or ambiguity may necessitate a supplemental paper-based agreement. Importantly, the loan product's terms and conditions include a number of clauses that imply the terms of the agreement could change. As discussed in section 5.1, legal professionals are concerned about smart contracts' ability to handle material change.

Figure 10. Smart Contracts' Potential Role in Mortgage Servicing
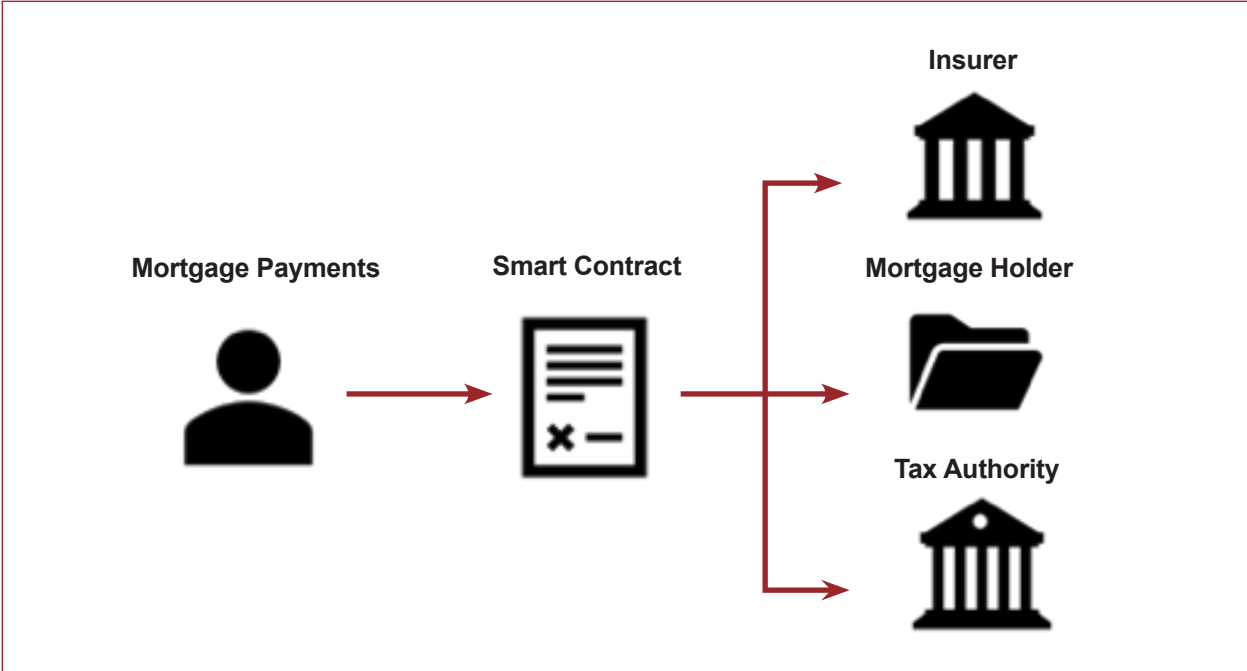
Source: Adapted from: Chamber of Digital Commerce (2016), "Smart Contracts: 12 Use Cases for Business & Beyond," Prepared by: Smart Contracts Alliance—In collaboration with Deloitte, December, pg. 28. Icon sources: Microsoft Office 365 ProPlus (subscription).

Annex:
How Smart Contracts Would Change Existing Microfinance Products

This Annex examines how select microfinance products would change if smart contracts are used for their deployment. The Annex is adapted from terms and conditions excerpts of two representative products, a weather index insurance (WII) policy and a mobile money-based, short-term unsecured loan. These products correspond to the insurance and consumer credit discussions contained in sections 7.2 and 7.3 of the note. Supply chain finance agreements, such as those discussed in section 7.1, are not examined in this Annex, as they are considerably more complex than the insurance and loan products reviewed below. For each product, the Annex illustrates the degree to which individual clauses are amenable to smart contract use. Table 3 outlines a color scheme used to facilitate the analysis.

Table 3. Contract Element Color Scheme

	Operational contract element conveying conditional logic which smart contracts are well-suited to capture.
	Contract element which may be fundamentally altered or eliminated if smart contracts are adopted.
	Element for which smart contracts must access an external data feed.[1]
	Clause for which natural language remains most appropriate. Smart contracts cannot easily or usefully express such clauses because they represent non-operational contract elements or entail discretion, judgement or ambiguity.

---

[1] "An oracle, in the context of blockchains and smart contracts, is an agent that finds and verifies real-world occurrences and submits this information to a blockchain to be used by smart contracts," (https://blockchainhub.net/blockchain-oracles/, accessed June 7, 2018).

A.1. Weather Index Insurance

Part I. Term Sheet for Rainfall Insurance Product

Crops covered	Any crop in the region		
Reference weather station	Center city weather station		
Index	Aggregate rainfall during the cover phases in mm.		
	If rainfall on a day is < 2 mm, it is not counted in the aggregate rainfall.		
	If rainfall on a day is > 60 mm, then rainfall in excess of 60 mm will not be counted in the aggregate rainfall.		
Definition of day 1	Calendar day in the month of June when cumulative rainfall for the month of June at reference station is observed > = 50 mm.		
	If above condition is not met in June, Policy invariably starts on July 1.		
Cover phase	**I**	**II**	**III**
Duration (days)	35	35	35
Strike (mm) <	95	110	95
Exit (mm) <	10	10	10
Notional ($/mm)	0.75	0.75	0.75
Policy limit ($)	75	75	75
Phase premium ($)	6.75	9.75	6.75
Data source	Center city meteorological department (CCMD)		
Settlement date	30 days after data are released by CCMD and verified by insurer.		

Smart contract will need to connect to weather station via external data feed

Pseudo example:
if (rainfall > 2 &
rainfall =< 60)
{index <- sum(rainfall)}

Pseudo example:
deficit <- 95 – index
payoutCalculator <-
function(deficit){
payout <- deficit*0.75

if(deficit > 85)
{payout <- 75}

if(deficit =< 0)
{payout <- 0}
return(payout)}

Explanation for the Terms Used

Term	Explanation
Reference Weather Station	The meteorological station where the observations for the purpose of claim settlement of the policy is made.
Index	Mathematical construct on the basis of which a policy is operationalized. It is the total rainfall received at the reference weather station in the policy period.
Cover Phase	These are the independent subperiods of the policy for which independent Strike, Exit, Notional, and Policy Limit are set. Each cover phase has a different index calculation.
Strike	The level of index below which the insured is compensated.
Exit	The level of the index below which the Insured becomes eligible for full Sum Insured under the Policy.
Notional	The amount of compensation that the insured receives when the index is below strike.
Phase Premium	Premium that the insured is required to pay for every unit of policy of respective phases, if he/she does not choose to take combined cover for all the phases.

Part II. Schedule Clauses

1. Scope of cover:

The Company hereby agrees, subject to the terms, conditions and exclusions herein contained, or otherwise expressed herein, to compensate the Insured for the cost of input, yield and/or increased operational costs of agricultural or non-agricultural economic activity as stated in the Policy, resulting from deviation of Observed Weather Index from Strike Index if such deviation is as stated in coverage within a specific geographical location and specified time period, subject to the maximum Sum Insured in the manner specified in Part I of the Schedule to this Policy.

Redundant with respect to the algorithmically-specified relationship.

2. Exclusions:

2.1. The Company shall not be liable to make any payment under this policy to the incurred by any in connection with or in respect of any expenses whatsoever incurred by any insured arising out of deviation in Weather Index resulting from:

(i) Ionizing radiations or contaminations by radioactivity from any nuclear waste from the combustion of nuclear fuel; or

(ii) The radioactive, toxic, explosive or other hazardous properties of any explosive nuclear assembly or nuclear component thereof.

2.2. The Company shall not be liable to make any payment under this Policy in connection with or in respect of any expenses whatsoever incurred by any Insured in connection with or in respect of any event leading to diminished agricultural or non-agricultural output/yield or increased operational costs, howsoever caused, other than on account of a deviation in weather parameters as stated in Part I of the Schedule within a specific geographical location and specified time period.

Unnecessary if contract assumes normal rainfall and executes only under deviations from deterministic threshold.

3. Claim procedure:

Upon the happening of any event giving rise to a claim under this Policy, the Insured shall deliver to the Company, irrespective of the date on which the event shall have occurred, but not earlier than the expiry of the Period of Insurance specified in Part I of the Schedule and not later than 60 days from the expiry of the Period of Insurance, a detailed statement in writing as per the claim form and any other material particular, relevant to the making of such claim along with duly completed claim form.

Smart contracts seek to reduce or eliminate claims filing by the customer.

4. Legal ownership:

During the Period of Insurance, the Insured shall possess all legal ownership rights with regard to the Property and / or Crop Cultivated. The Insured shall provide to the Company such title deeds and other documents as may be required by the Company for verification of his/her ownership over the Property and / or Crop Cultivated. The due observance and fulfillment of the above shall be a condition precedent for settlement of any claim under this Policy.

Could be handled by transferring rights to another entity and released as part of smart contract execution or expiry.

5. Incontestability and Duty of Disclosure:

The Policy shall be null and void and no benefit shall be payable in the event of untrue or incorrect statements, misrepresentation, mis-description or on non-disclosure in any material particular in the proposal form, personal statement, declaration and connected documents, or any material information having been withheld, or a claim being fraudulent or any fraudulent means or devices being used by the Insured or any one acting on his behalf to obtain any benefit under this Policy.

Unnecessary if contract assumes normal rainfall and executes only under deviations from deterministic threshold.

6. Reasonable care:

The Insured shall take all reasonable steps to safeguard the interests of the Insured against loss or damage that may give rise to a claim.

Non-operational, involves judgement

7.Material change:

The Insured shall immediately notify the Company in writing of any material change in the risk, in relation to the question in the proposal form and the declaration, and cause at his own expense such additional precautions to be taken as circumstances may require to ensure safe operation of the Insured items or trade or business practices thereby containing the circumstances that may give rise to the claim, and the Company may adjust the scope of cover and / or premium if necessary, accordingly.

It is unclear how smart contracts will handle material change clauses. Consistent with clauses 2.2 and 5, smart contract design may render this clause unnecessary.

8. Records to be maintained:

The Insured shall keep an accurate record containing all relevant particulars and shall allow the Company to inspect such record. The Insured shall within one month after the expiry of the Insurance Policy furnish such information as the Company may require.

Non-operational, involves judgement

9. Arbitration clause:

If any dispute or difference shall arise as to the quantum to be paid under this Policy (liability being otherwise admitted) such difference shall independently of all other questions be referred to the decision of a sole arbitrator to be appointed in writing by the parties to the dispute/difference, or if they cannot agree upon a single arbitrator within 30 days of any party invoking arbitration, the same shall be referred to a panel of three arbitrators, comprising two arbitrators, one to be appointed by each of the parties to the dispute/difference and the third arbitrator to be appointed by such two arbitrators. It is clearly agreed and understood that no difference or dispute shall be preferable to arbitration, as hereinbefore provided, if the Company has disputed or not accepted liability under or in respect of this Policy.

Smart contracts are intended to minimize challenges to contract execution and the need for arbitration. However, as argued in this note, smart contracts will not eliminate the need for dispute resolution (see: section 6.3). Regarding arbitration, jurisdictions will need to decide if arbitration is acceptable for smart contract disputes.

A.2. Mobile Money-based, Short-term Unsecured Loan

1. The Agreement

1.1. This Agreement sets out the complete Terms and Conditions (hereinafter called "these Terms and Conditions") which shall be applicable to the Account opened by you with the Bank.

1.2. These Terms and Conditions and any amendments or variations thereto take effect on their date of publication.

Non-operational expression of purpose and time of effectiveness

2. Acceptance of the terms and conditions

2.1. Before applying to open the Account via the Mobile Money System you should carefully read and understand these Terms and Conditions which will govern the use and operation of the Account.

2.2. If you do not agree with these Terms and Conditions, please click "Decline" on the Account Menu.

2.3. You will be deemed to have read, understood and accepted these Terms and Conditions: (i) Upon clicking on the "Accept" option on the Account Menu requesting you to confirm that you have read, understood and agreed to abide with these Terms and Conditions; and/or (ii) By using or continuing to use and operate the Account.

Pseudo example: ifelse(toc == "accept", send to credit eval, stop application)

2.4. These Terms and Conditions may be amended or varied by the Bank from time to time and the continued use of your Account constitutes your agreement to be bound by the terms of any such amendment or variation.

It is unclear how or if smart contracts can accommodate amendments.

3. Account opening

3.1. In order to open an Account with the Bank, you must be at least 18 years old and a registered and active Mobile Money Subscriber. The Bank reserves the right to verify with the MNO the authenticity and status of your Mobile Money Account.

3.2. You hereby agree and authorize the Bank to request the MNO for your personal information held by the MNO pursuant to the agreement between you and the MNO for the provision of MNO products and services and Mobile Money Service including your phone number, name, date of birth, ID or Passport Number and such other information that will enable the Bank to identify you and comply with the regulatory "Know Your Customer" requirements (together the "Personal Information").

3.3. You may open an Account solely by way of an electronic application made by you using your Equipment via the Account Menu.

3.4. Acceptance by the Bank of your application for an Account shall be done via SMS sent to the Mobile Phone Number associated with your Mobile Money Account.

3.5. The Bank reserves the right to decline your application for an Account or to revoke the same at any stage at the Bank's sole discretion and without assigning any reason or giving any notice thereto.

Smart contract must interact with multiple external data sources, including the bank, mobile money service, and MNO. Financial institutions likely need to use "permissioned" DLT platforms to comply with KYC standards (see: Box 1 and section 6.2).

4. Loan account

4.1. Subject to the approval of your application, the proceeds of the Loan shall be credited into your Account subject to any deductions on account of applicable Transaction Fees.

4.2. You shall make all payments due from you to the Bank in respect of the Loan and Transaction Fees using the Mobile Money Service and the System only unless otherwise agreed by the Bank in its discretion.

Smart contract must interact with mobile money service to facilitate loan payments

4.3. You shall repay the Loan within thirty (30) calendar days of the date of disbursement of the Loan.

4.4. In consideration of the Bank granting you the Loan, you shall pay the Bank a facility fee being 7.5% of the Loan amount (the "Facility Fee"). The Facility Fee shall be paid by you in arrears in addition to the Loan.

4.5. In the event that you do not repay the Loan in full within thirty (30) calendar days of the date of disbursement of the Loan, the Bank will automatically roll over any outstanding amount in respect of the Loan including the Facility Fee for a further period of thirty (30) calendar days

4.6. In consideration of the Bank forbearing to demand the immediate payment of the outstanding amount due in respect of your Loan and rolling over the same pursuant to Clause 4.6, you shall, in addition to paying the outstanding amount in respect of the Loan any outstanding Facility Fee, pay to the Bank a roll-over fee being 7.5% of the outstanding amount in respect of the Loan (the "Roll-Over Fee").

4.7. The Bank reserves the right to vary the terms of the Loan including the fees payable thereon from time to time having regard to the prevailing rules and regulations of the Central Bank and the policies of the Bank.

5. Variation and termination of relationship

5.1. The Bank may at any time, upon notice to you, terminate or vary its business relationship with you and close your Account and in particular but without prejudice to the generality of the foregoing the Bank may cancel credits which it has granted and require the repayment of outstanding debts resulting therefrom within such time as the Bank may determine.

5.2. You may close your Account at any time.

6. Dispute resolution, jurisdiction, and arbitration

6.1. You may contact the Customer Care Center to report any disputes, claims or Account discrepancies.

6.2. Any dispute arising out of or in connection with this Agreement that is not resolved by Customer Care Centre representatives shall be referred to arbitration by a single arbitrator to be appointed by agreement between the parties or in default of such agreement within 60 days of the notification of a dispute, upon the application of either party, by the Chairman for the time being of the Institute of Arbitrators.

6.3. To the extent permissible by Law, the determination of the Arbitrator shall be final, conclusive and binding upon the parties hereto.

6.4. This Agreement shall be governed by and construed in accordance with the laws of the country.

Pseudo example:
loanAmount <- x
repayDate <- t + 30
amountDue <-
loanAmount*1.075
outstanding
<- amountDue -
paymentsMade

if (date = repayDate
& outstanding > 0)
{outstanding <-
outstanding * 1.075

Smart contracts are intended to be self-executing and immutable. Though the ability to exit the agreement at any time seems contrary to the purpose of smart contracts, contract code can potentially encompass a party's unilateral decision as a trigger.

Smart contracts are intended to minimize challenges to contract execution and the need for arbitration. However, FCP standards will require dispute resolution options (see: sections 6.1 and 6.3). Regarding arbitration, jurisdictions will need to decide if arbitration is acceptable for smart contract disputes.

Endnotes

1. World Bank Group (WBG) (2017a), "Distributed Ledger Technology (DLT) and Blockchain," Finance, Competitiveness & Innovation Global Practice: Fintech Note No.1.

2. Blockchain is a form of DLT. See WBG 2017a for an in-depth discussion of DLT and blockchain.

3. Deloitte (2019), Deloitte's 2019 Global Blockchain Survey: Blockchain Gets Down to Business. Deloitte Insights.

4. Deloitte 2019.

5. Deloitte 2019.

6. Szabo comprehensively defines smart contracts in the opening paragraph of his 1994 paper: "A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs." See: Szabo, Nick (1994), "Smart Contracts," http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

7. Szabo, Nick (1996), "Smart Contracts: Building Blocks for Digital Markets," http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html, accessed March 19, 2017.

8. Szabo emphasizes the security aspects of smart contracts, explaining that they involve "using cryptographic and other security mechanisms" to "secure many algorithmically specifiable relationships from breach…eavesdropping or malicious interference." See: Szabo, Nick (1997), "Smart Contracts: Formalizing and Securing Relationships on Public Networks," First Monday, Volume 2, Number 9 – 1, September, http://firstmonday.org/ojs/index.php/fm/article/view/548/469, accessed March 19, 2017.

9. In this context, Boolean logic refers to conditions that take on two possible values, true or false, and compel differing actions based on the value.

10. Clack, Christopher D., Vikram A. Bakshi, and Lee Braine (2017: 2), "Smart Contract Templates: foundations, design landscape and research directions," Barclays Bank PLC.

11. In a useful analogy, Szabo illustrates these characteristics by describing the "humble vending machine" as a "primitive ancestor of smart contracts," which protects property and executes a transaction in an immutable, transparent fashion only once the requisite change has been dispensed. See: Szabo (1996).

12. Stark, Josh (2016), "Making Sense of Blockchain Smart Contracts," Coindesk, June 4, https://www.coindesk.com/making-sense-smart-contracts/, accessed April 25, 2018.

13. Stark (2016)

14. Chamber of Digital Commerce (2016), "Smart Contracts: 12 Use Cases for Business & Beyond," Prepared by: Smart Contracts Alliance—In collaboration with Deloitte, December.

15. Raskin, Max (2016), "The Law and Legality of Smart Contracts," 1 Georgetown Law Technology Review 304 (2017), September 22, pg. 307.

16. International Swaps and Derivatives Association (ISDA) (2017), "Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective," August, pg. 22.

17. European Bank for Reconstruction and Development (EBRD) (2018), "Smart Contracts: Legal Framework and Proposed Guidelines," September, pgs. 12-13.

18. For an overview of DLT and blockchain, see: WBG (2017a), FinTech Note No. 1. Satoshi Nakamoto is the pseudonym of the unidentified author of the 2008 white paper entitled, "Bitcoin: A Peer-to-Peer Electronic Cash System."

19. Chamber of Digital Commerce (2016: 3)

20. U.S. Commodity Future Trading Commission (CFTC 2018), A Primer on Smart Contracts, LabCFTC, November 27, https://www.cftc.gov/PressRoom/PressReleases/7847-18, accessed March 14, 2019.; Clack, et al. (2017); EBRD (2018); ISDA (2017).

21. Szabo acknowledges in the 2016 white paper that financial institutions were already implementing forms of smart contracts prior to his 1994 conceptualization without labelling them as such (Chamber of Digital Commerce 2016: 3). As one example, banks have long used automated computing procedures to pay interest on savings accounts based on the varying balance in the account and according to the payment frequency and interest rate specified in the agreement. Such an arrangement certainly represents "a computerized transaction protocol that executes the terms of a contract (Szabo 1994)." However, blockchain-based smart contracts attempt to limit the control that intermediaries have over the performance of the agreement. In the case of the interest-bearing savings account, although the bank specifies certain contractual elements algorithmically, it still monopolizes the validation and execution process.

22. Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone (2018), Blockchain Technology Overview, National Institute of Standards and Technology: U.S. Department of Commerce, October, pg. 32.

23. International Financial Corporation (IFC) (2019), Blockchain: Opportunities for Private Enterprises in Emerging Markets, January, pg. 71.

24. Capgemini Consulting (2016), "Smart Contracts in Financial Services: Getting from Hype to Reality," October 11; Chamber of Digital Commerce (2016).

25. North, Douglass (1990), Institutions, Institutional Change and Economic Performance, Cambridge: Cambridge University Press, pg. 27. For other prominent conceptions of transaction costs, see: Coase, R.H. (1937), "The Nature of the Firm," Economica, New Series, Vol. 4, No. 16. (Nov.), pp. 386-405; Coase, R.H. (1960), "The Problem of Social Cost," The Journal of Law & Economics, Vol. 3 (October), pp. 1-44; Dahlman, Carl J. (1979), "The Problem of Externality," The Journal of Law & Economics, Vol. 22, No. 1 (Apr., 1979), pp. 141-162.; Williamson, Oliver E. (1981), "The Economics of Organization: The Transaction Cost Approach," American Journal of Sociology, Vol. 87, No. 3 (Nov., 1981), pp. 548-577.

26. For North, transaction costs are reflective of the informational asymmetries and resulting uncertainty intrinsic to economic exchange. To cope with this uncertainty, societies develop institutions, which North defines as the "humanly devised constraints that shape human interaction (North 1990: 3)." Institutions, which can be formal (e.g., explicit rules) or informal (e.g., conventions), reduce, but do not eliminate, transaction costs. Indeed, they are costly to maintain and contribute to transaction costs themselves, but without them, impersonal exchange, the primary form of economic activity in modern economies, would be extremely difficult.

27. Szabo (1996, 1997)

28. Szabo (1997)

29. Cong, Lin Willian and Zhiguo He (2018), Blockchain Disruptions and Smart Contracts, The Review of Financial Studies, Volume 32, Issue 5, May 2019, Pages 1754–1797; Gans, Joshua S. (2019), The Fine Print in Smart Contracts, NBER Working Paper No. 25443.

30. Buterin, Vitalik (2013), "A Next-Generation Smart Contract and Decentralized Application Platform," https://github.com/ethereum/wiki/wiki/White-Paper, accessed March 19, 2017; Chamber of Digital Commerce (2016); Szabo (1996, 1997)

31. Szabo summarizes this future vision in his forward to the 2016 Chamber of Digital Commerce white paper: "The smart contract goes beyond enterprise business solutions – in fact my personal favorite and most exciting type of smart contract is constructed in peer-to-peer environments, from simple natural language by individuals to operate between individuals. This movie will get even more exciting when machine-to-machine adoption takes shape at the intersection of blockchain, artificial intelligence and the Internet of Things (Chamber of Digital Commerce 2016: 3)." Additionally, see: Christidis, Konstantinos and Michael Devetsikiotis (2016), Blockchains and Smart Contracts for the Internet of Things, IEEE Access, April 23.

32. Cornell Law School, "Contract," Legal Information Institute, https://www.law.cornell.edu/wex/contract, accessed April 27, 2018.

33. Computers only read binary (1s and 0s). Multiple behind-the-scenes steps are often required to translate a high-level programming language into something the computer can work with.

34. Szabo (1996, 1997)

35. Raskin (2016); Wan, Amy (2017), "ICO and Smart Contract Law with Amy Wan," Crypto 101: The Average Consumers Guide to Cryptocurrency, Podcast episode, December 12.

36. Pisa, Michael and Matt Juden (2017), "Blockchain and Economic Development: Hype vs. Reality," Center for Global Development: Policy Paper 107, July, pg. 15.

37. CFTC (2018: 5)

38. Chamber of Digital Commerce (2016); Raskin (2016)

39. Raskin (2016)

40. Chamber of Digital Commerce (2016)

41. Chamber of Digital Commerce (2016); Clack et al. (2017); EBRD (2017); ISDA (2017), Stark (2016)

42. ISDA (2017)

43. World Bank Group (WBG) (2017b), Good Practices for Financial Consumer Protection, Finance & Markets Global Practice, pg. 33.

44. WBG (2017b: 39)

45. WBG (2017b: 49-52)

46. WBG (2017b: 34-37)

47. WBG (2017b: 34)

48. WBG (2017b: 23)

49. Financial Action Task Force (FATF) (2012-2019), "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations," Paris, France.

50. Financial Action Task Force (FATF) (2013-2017), "FATF Guidance: Anti-money laundering and terrorist financing measures and financial inclusion, with a supplement on customer due diligence," Paris, France.

51. FATF (2012-2019).

52. Financial Action Task Force (FATF) (2019b), "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," Paris, France.

53. Financial Action Task Force (FATF) (2019a), "Draft Guidance on Digital Identity," Paris: France, pg. 23.

54. Financial Action Task Force (FATF), Public consultation on FATF draft guidance on digital identity, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html, accessed December 1, 2019.

55. EBRD 2018: 15

56. EBRD 2018

57. Analysts have also discussed digital identity as a blockchain use case. To the extent that blockchain-based digital identities are widely adopted, they could be integrated into smart contract facilitated transactions. For a discussion of blockchain applications for digital identity, see: World Bank Group and Digital Impact Alliance (WBG and DIAL) (2018), Technology Landscape for Digital Identification.

58. IFC, MSME Finance Gap Database, October 2018 update.

59. World Bank Group (WBG) (2018), "How Technology Can Make Insurance More Inclusive," Finance, Competitiveness & Innovation Global Practice: Fintech Note No.2.

60. Capgemini (2016); Haleem, Aneeza (2018), "Smart Contracts for Smarter Lending," MBA Insights, June 20, https://www.mba.org/publications/insights/archive/mba-insights-archive/2018/smart-contracts-for-smarter-lending, accessed June 5, 2018.