U.S. Patent Granted - US10915873B2
(E.U. Pending)

BLOCFONE: A CENTRALISED COUNTERPARTY THAT LEVERAGES A DISTRIBUTED PUBLIC LEDGER, PRIVATE SIDECHAINS AND SMART CONTRACTS WITH ORACLES TO PROVIDE VOICE, DATA & TEXT, AS WELL LOCAL MARKETPLACE OFFERS

White Paper

blocfone®, fonecoin® and FON®

E. R. Martin

BLOCFONE: A CENTRALISED COUNTERPARTY THAT LEVERAGES A DISTRIBUTED PUBLIC LEDGER, PRIVATE SIDECHAINS AND SMART CONTRACTS WITH ORACLES TO PROVIDE VOICE, DATA & TEXT

U.S. Patent Granted - US10915873B2. E.U. Patent Pending - EP3542333

Eric Richard Martin
JM, Emory University School of Law
Spring 2016

ABSTRACT: Consumers of mobile voice, data and text services are constantly faced with connectivity issues when crossing into and out of service provider coverage areas. There are 2 main reasons: 1) hardware: out-of-range of a cell tower, hotspot or satellite and/or missing frequency/band on mobile device and/or traffic capacity; and 2) commercial: legal terms and conditions with a designated provider do not provide connectivity despite availability of connectivity, and cross-border (international) billing and payment complexity. Technology, on the other hand, is not a main issue per se, as nowadays mobile devices are capable of connecting to voice, data and text services anywhere anytime and global payment platforms already exist (PayPal, credit cards, etc.). This paper endeavors to explore the use of Bitcoin's distributed public ledger technology framework, 'blockchain', combined with private ledgers, 'sidechains', to govern 'smart contracts' employing performance monitoring technology 'oracles'. A trusted central counterparty in the form of a 'private sidechain' is setup to essentially break down competitive commercial barriers while offering consumers seamless and unified global roaming, local marketplaces and simplified payment procedures while minimizing costs and risk to service providers.

Introduction

The demand for mobile voice, data and text services is increasing rapidly. As of November 2015 there were an estimated 7.4 billion worldwide mobile subscriptions projected to be 9.1 billion by 2021, with a projected 45% increase in mobile traffic growth (Ericsson Mobility Report, November 2015). Subscribers are served by approximately 800 operators worldwide (GSM Association, 2016).

According to the GSM Association, the term roaming is defined as the ability for a customer to automatically make and receive voice calls, send and receive data, or access other services when travelling outside the geographical coverage area of the home network, by means of using a visited network.

Roaming is technically supported by mobility management systems, authentication of active accounts upon switching from one network to another, and billing procedures to support delivery of services to subscribers across a range of networks.

If the visited network is in the same country as the home network, this is known as national roaming. If the visited network is outside the home country, this is known as international roaming. Lately, the term global roaming has been gaining traction in the community.

In all cases, roaming requires a 'handoff' from the home network to the visiting network, creating a provider-to-subscriber relationship. It is not uncommon for a visiting network within the same country to be a direct competitor of the home network provider, less so when crossing international borders. Regardless, the consumer is nonetheless a formal subscribing customer to only one provider within the home network, and becomes indirectly bound to the terms and conditions of the visiting network provider via the home network provider's contract with the subscriber. In parallel, the home network provider engages contractually with a web of visiting network providers in order to maximize

coverage for its subscribers. The contractual terms between providers cover various items from authentication procedures, security, service level agreements, performance guarantees, adjudication procedures, and of course consideration such as service and administrative fees in order to provide continuity of service to the home network's subscribers. These costs are shared at wholesale rates among providers and typically absorbed, at a premium, by subscribers.

The time, money, technology, processes and collaboration required to develop provider-to-provider partnerships and agreements leading to accessible networks by a single subscriber by default puts the subscriber in a disadvantageous position. As such, subscribers lack service even where coverage exists, are forced to accept lower levels of service due to provider-to-provider Service Level Agreements, and most importantly charged exorbitant fees lacking in transparency for the privilege of accessing visiting networks worldwide. In turn, and for various technical reasons -- many of which are now legacy -- and evolving quickly as smart phones improve connectivity functionality, subscribers who tend to roam a lot, particularly international travelers, mitigate connectivity risk and costs by 'playing complex games' carrying multiple phones, multiple SIM cards, accessing Wifi Hotspots, purchasing 'travel packages', etc. Not only is this process time consuming and costly, it often fails in practice leaving subscribers exhausted in an attempt to maintain connectivity, which is now being propagated across the globe as a 'basic

service'. In developing countries, mobile voice, data and text can be the only channel to access information without 'hard lines' delivered to home or office.

The response to this pain is simple. Visiting network providers should provide direct services to subscribers on their mobile device within the visiting network, and to cut through all of the indirect provider-to-provider red tape. However, this will never happen (at least not in the foreseeable future) because the user experience would fall flat and it would require all 800+ operators around the globe to change their systems and procedures, and voluntarily decide to lower prices to subscribers, else agree to alter the operating model to open up competition. Just imagine each time a subscriber moves from state to state in the U.S., in order to maintain continuity of service, subscriber would need to 'sign up' or 'sign in', enter personal information, payment methods, and accept terms and conditions with each and every visiting network. No thanks, I'll wait for the Wifi at the next Starbucks (except I don't like this either due to privacy concerns). From a provider perspective, the administrative burden would be enormous as 800+ operators would need to agree to standard operating procedures for direct interaction with subscribers, including billing procedures, and even know-your-customer requirements. When these decisions are taken, then markets would be required to wait while operators embed these standards into enterprise systems end-to-end. Granted, in the U.S., the pain is less roaming from state to state, as fierce competition has brought pricing down to 'all you can consume' style plans, however,

'good coverage' is still an issue when the best visiting network available is not connected to a subscriber's home network provider. Outside the U.S., the pain proliferates as subscribers move freely from country to country in the E.U., within countries throughout Africa and Asia, and even worse for populations whose subscribers prefer pre-paid plans versus contracts which do not allow real-time billing for 'additional services' (i.e., entering a roaming network) as contract plans typically do.

Therefore, the most feasible solution is one that is disruptive, neutral and trusted, and is given the opportunity to grow organically beginning with niche markets in the short term (international roaming), while long term moving providers over time to fundamentally change their operating models to respond to a global market seeking a 'simple' unified solution. There is an argument that a disruptive solution is a 'solution seeking a problem' because providers can simply lower prices and update network sharing agreements. However, consider years ago the concept of toll calls state-to-state and exorbitant prices for 'true' long distance and international calling. At any time the markets could have reduced pricing as infrastructure was already capitalized, instead it required the disruptive use of electronic email and mobile phones that finally 'forced' pricing down to current levels for hard lines. Altruism is not in the 'top 5' of the business world priorities. This is only one facet, of course, which will be described later in the paper but worthy of considering up front.

One such disruptive approach utilizes innovative technology platforms and methodologies including blockchain enabled by smart contracts. Both components have garnered significant interest by the financial and banking communities in recent years. While the origins of these technologies date back more than 20 years, a search on the US Patent & Trademark Office (April 2016) website reveal only two patents and 33 applications that reference blockchain, and zero patents and 3 applications that reference smart contract. As a comparison, over 8,700 patents were returned by a comparable platform search term 'SQL Server', and this would be 'scratching the surface'. Therefore it is important to recognize that this nascent technology and industry is evolving quickly, and references to terms, structures, architecture, definitions, etc. may be redefined at any given moment, or not fully agreed within the community itself. Additionally, for every bleeding edge solution, there seems to be an equal set of new challenges unearthed and it is therefore understood that new methodologies may surface at any time and gain more traction in the markets than current methodologies currently undergoing detailed discovery and testing.

The following section will describe relevant technologies, platforms and standards through use case scenarios being explored in the financial and banking communities, and will avoid as much as possible any deep dives into the technical infrastructure itself or financial product architecture, focusing instead on interdependencies of the business case, centralised counterparty concept, secure

and trusted distributed network (blockchain), smart contracts with oracles and parallel transaction systems to facilitate FX payments (sidechains) that glue business, standards, and technology propositions together, and specifically to convert voice, data and text to a direct provider-to-consumer offer, bought and sold anytime anywhere by individual subscribers. Following this analysis is the proposed structure of a solution called blocfone™.

Background Scenarios in Financial and Banking Communities

Central Counterparty (CCP) for Mitigating Risks Associated to Derivatives Markets

As found in the Glossary of the Committee on Payments and Market Infrastructures (CPMI) website at https://www.bis.org/cpmi/publ/d00b.htm:

A central counterparty interposes itself between counterparties to contracts traded in ... financial markets, becoming the **buyer to every seller and the seller to every buyer** thereby ensuring the performance of open contracts.

In his 2013 white paper entitled Understanding Derivatives: Markets and Infrastructure Central Counterparty Clearing, Robert S. Steigerwald, senior policy advisor, financial markets, Federal Reserve Bank of Chicago outlines the legal

framework that essentially makes a CCP viable, also referencing the Glossary of the CPMI, including:

Novation: A process through which the original obligation between a buyer and a seller is discharged through the substitution of the CCP as seller to the buyer and buyer to the seller, creating two new contracts; and

Open-offer system, where a CCP is automatically and immediately interposed in a transaction at the moment the buyer and seller agree on the terms.

Mr. Steigerwald explains how the CCP becomes a substituted counterparty to a preexisting, legally enforceable contract: "The answer to that question turns on the law of contract in the jurisdiction (or jurisdictions) in which the CCP operates. Most modern clearing arrangements depend on one of two legal doctrines to support the interposition of the CCP as common counterparty to all trades—novation and open offer.

Mr. Steigerwald further explains: "Because the CCP becomes a principal to all trades with its clearing members, it must carry out the future performance obligations to which they initially agreed. The CCP acts on its own behalf (as principal) and for the mutual benefit of its clearing members by imposing risk management policies and establishing operational processes to support the settlement of transactions cleared through the CCP. It also plays a fundamental role in responding to and resolving clearing member defaults and other circumstances that threaten the orderly operation of the clearinghouse."

The purpose of referencing a CCP up front, and specifically against the backdrop of the most recent financial crisis is to point out the inherent benefits of creating a platform and processes that reduce complexity and increases transparency, especially when mitigating systemic risk that can be significantly impacted by complex financial products such as derivatives. Additionally, to point out the legal framework that makes it possible to impose a neutral party who is "both buyer and seller". Of course, nothing is bulletproof, and by concentrating risk in and of itself creates risk, the application of a CCP is further enhanced by decentralized blockchain technology and smart contracts that chip away at the risk of non-performance as will be explained later in the paper.

It is also important to note upfront that it may be considered contradictory to include the use of a CCP with blockchain technology, as the blockchain methodologies for creating a 'trustless' system can actually replace the need for a CCP. I disagree, in real life scenarios these two complement one another. This will be discussed further. It is also important not to confuse 'counterparty' with Counterparty, a technology company that offers solutions on top of the Bitcoin blockchain with overlapping general concepts of the financial definition of counterparty.

Blockchain for Selling Options

Before explaining the use case for selling options on blockchain, it is important to explain blockchain itself. As this technology is currently 'bleeding edge' there are not many 'easy to understand explanations' in the universe today to my knowledge, however, there is white paper that does an excellent job and references terms which I have adopted: Ethereum: A secure decentralized transaction ledger, Final Draft – Under Review by Dr. Gavin Wood, Co-Founder & Lead, Ethereum Project (www.ethereum.org).

I will try to explain in these terms with analogies just enough to advance the purpose of this paper. Blockchain is basically a data store based on references to stored data by a trusted public electronic general ledger. Like an individual trusts the general ledger of his/her bank account transactions, a debit for buying groceries on the buyer side triggers a credit for selling groceries on the seller side. The ledger itself does not hold the groceries of course, and assuming the transaction is proven valid over time, the ledger simply references a transaction where groceries left a shelf in the store (and on an inventory system) and perhaps restocked into a refrigerator at home. Validation happens electronically when systems balance automatically and then when humans look at the ***their own personal ledger (e.g., account statements)*** to determine finally if transactions are valid or not (e.g., fraud), as well as simply reaching into the refrigerator and finding food of course. Buyer and seller's personal ledgers (statements, reconciliation systems, etc.) are essentially the 'centralised private ledgers' when compared to a public,

decentralized blockchain approach. Blockchain is different in that it is a single and transparent general ledger into which all parties have a view, not to every private detail, but to ensure validity of transaction references starting from the root, the empty shelves stocked for the first time if you will, called the "genesis block", to the leaf (the current block containing the latest batch of transactions), and forever linked together by a computer 'tree' structure based on an agreed upon scheme. This is a very important distinction because trust and transparency go hand in hand. An individual trusts his/her bank because statements are delivered regularly and expose transactions, and when transactions are deemed incorrect, banks agree to fix them contractually. Behind the scenes, banks worry and investigate fraud, and trust their customers when reporting incorrect transactions based on a number of criteria that seeks to reveal exceptional fraudulent behavior. The bank then has control over the centralised ledger. Blockchain, however, must remain neutral and secure in order for trust to occur on both sides of any transaction. At any given moment in time, almost in real time (not 'regularly' such as monthly statements) whether one block of transactions or millions of blocks chained together, the final [most current] state must be accepted by all parties (the canonical state).

To garner acceptance and maintain trust of the canonical state (which is changing all the time), blocks building upon other blocks of transactions can never be changed once accepted, and a blockchain as a whole must be valid and trusted at all times, based on a process to weed out unacceptable blocks of transactions. Back

to the grocery purchase example, if an individual determines a credit card charge for groceries was incorrect, the bank decides whether to credit the customer or not, and will reverse the charge or not. The transaction remains in the bank's database history, one for the original charge, and one for reversing the charge, and a new entry crediting a write-off. Trust is contractual combined with goodwill among the bank and customer. Blockchain provides a methodology to build trust electronically (no human interaction) and neutrally; there is no 'bank' or 'fraud department' making final decisions on the validity of changes to the blockchain, because it never changes, blocks are added and the chain grows. Instead, blockchain is considered 'trustless' by distributing this responsibility to everyone and no one by replicating the blockchain on multiple electronic 'servers' and allowing no additional blocks added to the tree unless consensus occurs to add a block among all valid copies of the blockchain based on an agreed upon methodology. This consensus is built upon a system called 'proof of work', and is conducted by 'miners' (i.e., everyone who holds a copy of the blockchain) based on an incentive system. Once a 'proof of work' is complete, a block is added and updated to every copy as the latest canonical state. Essentially, I like to think of any blocks rejected (e.g., hackers copies) as being shamed off the island based on the consensus of all miners. Much content can go into describing the incentive-based system for miners that promotes trust and accuracy, but for the purpose of this paper the assumption is that the proof-of-work consensus based process is ***the*** reason the benefits of a decentralized public ledger

system exists, and why it is important to explore opportunities within various markets and use cases. Otherwise, technically speaking, utilizing blockchain technology versus existing centralized database technology becomes nothing more than a 'fit-for-purpose' analysis under 'business-as-usual' conditions.

Why all the fuss to setup a decentralized version of a centralised system already embedded in the ecosystem? Because a public general ledger is not really tracking 'grocery sales transactions', it is tracking the transfer of electronic value, the consideration that changes hands when a buyer buys groceries and a supermarket makes a sale, or when a seller sells options and a buyer buys options to purchase shares. Unlike the former where full consideration is exchanged and goods can be 'touched and consumed' instantaneously, the latter involves a promise to pay upon a pre-defined event or expiration of the option, potentially a down payment in the amount of a margin percentage calculation held by a custodian, and includes all risks associated to potential default of one or more parties when an option is finally settled. Settlement whether instantaneously or based on a promise to pay in the future occurs via the electronic version any typical transfer of money, whether using keys to the vault to retrieve gold bullion to hand deliver to the seller, handing bills/notes backed by central banks to seller, to executing wire transfers, etc. in return for goods, services, financial gains, etc. In the blockchain, the end-to-end process is electronic (i.e., humanless and supposedly cheaper and faster, and no gold bullion waiting in the vault). To pass electronic value from one party to another

requires secure, sophisticated cryptographic technology (the keys to the vault so to speak) that only counterparties share, are used to effectuate a transfer of value, to then be validated and recorded to the blockchain via the 'proof of work' process, the transaction settled is and remains in full view of the blockchain community for eternity. Bitcoin is an example of a true electronic currency, a cryptocurrency testing the waters in a live deployment of a decentralized Bitcoin blockchain. There can be an unlimited number of cryptocurrencies and blockchains. For the purpose of this paper, an assumption is maintained that planet earth only requires one public decentralized ledger and Main currency (Bitcoin) and can include private centralised ledgers to conduct its purposes but still linked to Bitcoin for the ultimate and unified transfer of electronic value. But it future practices, I predict branded cryptocurrencies will emerge for specific purposes (e.g., for my blofone™ invention there could be fonecoin™ the electronic currency used to buy and sell mobile voice, text and data services, as well as easy use on local marketplaces) and these branded cryptocurrencies would be backed via private sidechains effectuating the exchange of value in either existing currencies (USD, EUR, GBP, etc.) or even commonly accepted cryptocurrencies (Bitcoin), depending on the end-user customers' (buyer and seller) preference.

Smart Contracts

Up to this point, I have summarized how a centralized counterparty can take ownership of contractual obligations by becoming both 'buyer and seller' to promote efficiencies and provide transparency to a trading system in favor of minimizing risks. I have also summarized an innovative decentralized public transaction general ledger framework (blockchain) combined with a secure electronic cryptocurrency example that is live and being used in markets (Bitcoin) to exchange consideration end-to-end within a trustless (i.e., no humans, and no trust required because the system is essentially foolproof) platform.

In between taking ownership of obligations and enabling exchange of consideration, performance (in the legal contract sense) of the obligations must occur. This process can also be embedded electronically because the blockchain framework is essentially an open database, and anything that can be stored in a database (account balances, names, descriptions, due dates, payment amounts, payment timing, expiration dates, etc.) can be monitored. Technically, any data stored can also be referenced back to, or 'packaged with' the consideration exchanged. For example, in a Bitcoin exchange, relevant data elements can be referenced within the transaction and stored forever within a blockchain inside a block as a transaction, finally approved by miners and recorded by the consensus driven proof of work process. The paper version is the stamped and signed title documents and mortgage security documents filed at the Secretary of State's office, scanned and finally available via the Internet for view, download, print, etc..

Further, any condition 'if x / then y' that can be tracked electronically can also be associated to blockchain transactions and can trigger actions (e.g., payment upon delivery, margin calls, commence foreclosure proceedings, repo the car, etc.) when an event monitor returns a positive response.

Here is an example of how to embed contractual terms into an electronic smart contract using an option contract example (reference Nick Szabo's Papers and Concise Tutorials, http://szabo.best.vwh.net/contractlanguage.html):

"In this American option, the Holder has the right to buy for $20 (the option strike price) per share one round lot (100 shares) of XYZ Corp on or before the last trading day of August. These kinds of contracts are called "derivatives" because the call option is derived from the underlying right (here a stock).

```
callOptionAmerican (rightA="1 round lot XYZ Corp.",
                    rightB="$2,000/lot",
                    time="end of trading on last trading day of August") =
        when beforeTime(time)
                when choiceOf(Holder)
                        to Holder rightA with to Counterparty rightB
        when afterTime(time)
                terminate
```

Here is another example using a famous 13th century "dry exchange" damages calculation:

```
        counterpartySecurity =  pledge(allGoods(Counterparty))
        also cosignerSecurity = pledge(allGoods(co-signer))
        then
payment1() =
        when beforeTime("Kalends of September 1275")
                to Holder in Byzantium "53 hyperpers"
                terminate
payment2() =
        when breachedPerformance(payment1)
                to Holder in Genoa "53*11 = 583 shillings"
                terminate
payment3() =
        when breachedPerformance(payment2)
                to Holder in Genoa "2*583 shillings"
                terminate
payment3() =
        when breachedPerformance(payment3)
                when choiceOf(Holder)
                        to Holder in Genoa foreclose(counterpartySecurity, penalty)
                        terminate
                when choiceOf(Holder)
                        to Holder in Genoa foreclose(cosignerSecurity, penalty)
                        terminate
                continue
```

While the format is clearly machine driven syntax, an adept legal professional can see embedded within the computer code the terms and conditions of an agreement. When packaged as a whole and referenced by a blockchain transaction the Smart Contract is formed, and together with the exchange of consideration such as Bitcoin the Smart Contract becomes effective. Computers then begin the process of monitoring performance, recording events and triggering actions. No longer are humans needed, nor the trust associated to human interaction (caveat, never 100% of course). The role of attorney becomes less about facilitating and ensuring performance, even through adjudication procedures, and more about developing templates that can be converted to computer language and

incorporated into smart contracts that can be executed automatically and electronically.

As stated earlier, the assumption is that only Bitcoin is in scope as the public cryptocurrency. Like any large enterprise technology implementation, platform changes take much consideration and time, and therefore the Bitcoin blockchain is not an 'end all' platform. Many tasks, including monitoring performance of smart contracts, require off-chain solutions, hence, my prediction that branded cryptocurrencies will emerge supported by trusted private sidechains tailored to include relevant smart contracts.

Oracles and Sidechains

Monitoring performance of clauses within a smart contract that utilizes Bitcoin's blockchain requires off-chain solutions (technically, until it can be built-into the 'one and only one' accepted blockchain like Bitcoin). The Bitcoin implementation in its current state simply does not include the 'functionality' necessary beyond the basics. These solutions, to be consistent with the 'trustless' based notion of a public decentralized ledger and payment platform, requires the use of oracles. Oracles are nothing more than computer programs that 'reach out' to external services automatically, and if the response triggers an action to commence in a smart contract clause, that action is commenced. An example using options,

assume an option strike price occurs at $x. An oracle in place to monitor performance of the smart contract covering this transaction would observe external trusted market pricing systems such as Bloomberg, and when the strike price $x exists would trigger a Bitcoin transaction to complete.

This process extends to other applications. Imagine a car with a smart key that is associated to a car loan. If an oracle determines that a loan payment is in default, then the smart key may be triggered to disable the car and note its location for a repo representative to pick-up.

Even further application consider beneficiaries in wills. A smart will may include an associated oracle to reach out to mortality databases, and if a deceased response is returned automatically trigger a beneficiary clause to move Bitcoin from the deceased's account to the beneficiary's account.

Oracles seem quite straight forward, except that the potential to undermine the trust of the public decentralized transaction ledger, Bitcoin, rises significantly as self-interested humans programming and interacting with oracles can cause triggers and changes to the blockchain from 'behind the curtain', the exact opposite of the intention of blockchain technology.

In response to this conflicting risk, a concept to implement private blockchains, or sidechains running in parallel to and directly integrated with (or not) blockchains such as Bitcoin is being considered within the community. In theory, if necessary off-chain tasks must be included to provide value to an end-to-

end solution (e.g., oracles monitoring smart contracts), then it must include the same level (or as close as possible) of trust as a public blockchain itself. Otherwise I refer back to the 'fit for purpose' technology test in a 'business as usual' environment. Trust is essential. Alternatively, if Bitcoin is forever seared as the foundational cryptocurrency in the world market then all features and functions can eventually be built directly into the Bitcoin platform. Obviously this is not a feasible approach in a foreseeable view, and instead a balance will need to be found over time. In any case, any private sidechain would require its own incentive-based proof-of-work process to garner the same (or close enough) level of trust in an end to end value chain. For the financial and banking industry, this is more significant challenge than, say, for websites that provide smart wills to pass along Bitcoin upon death. Using the options example, and assuming either Bitcoin is the exchange of value, or a sidechain cryptocurrency is developed for the options market. If it is a private sidechain, even though distributed like a public blockchain, it is still a 'private self-interested group' – a subset of all humans on planet earth seeking to exchange value, similar to the community of "Too Big to Fail Banks" for example. There are emerging technologies such as www.truthcoin.com -- notice even the branding has to indicate something about trust – attempting to solve this dilemma.

In summary, the previous discussion focused on foundational structures and processes to convey the emerging interest in utilizing decentralized public general

ledger technology. The basis of all attributes of any end-to-end real life solution is trust. A centralized counterparty brings trust to the process by becoming 'buyer and seller'. Blockchain technology brings trust to the process with its public access and technical architecture combined with its trust-seeking incentive-based proof-of-work process. Oracles bring trust to the process by automating the monitoring of performance and triggering contractual obligations and recourse. Private sidechains bring trust to the process by expanding the functionality of dependent, but not fully functional public blockchains using similar trust-based methodologies.

As will be discussed in the following section regarding the specific use-case for voice, data and text, not all foundational structures may be required. In fact, there are competing views as to which override, or are redundant, or are simply not needed in favor of conventional non-public, centralized systems already in place.

Blocfone – a Solution to a Real Problem

Before beginning the discussion of the use of blockchains, sidechains, oracles, and Bitcoin as an efficient methodology for serving global roaming subscribers to voice, data and text services, a summary of the regulatory environment is in order.

According to the GSM Association, "regulators and policymakers have communicated significant concerns regarding consumer "bill- shock", transparency, and have focused on higher international mobile roaming prices. However, the resulting dialogue between regulators, policymakers and industry has at times

become challenging due to the significant economic, commercial and technical complexity of international mobile roaming." (Information Paper, Overview of International Mobile Roaming, 25 June 2012).

The Information Paper further outlines the mechanics of roaming, tariffs, and essentially concludes that "operators compete through a process of tariff innovation." (p. 8), and that the "costs directly associated with these elements and providing roaming services include:

- Reaching and maintaining bilateral roaming agreements
- Roaming specific communications and marketing costs
- Implementation of technical infrastructure, testing and updating
- Payments to roaming clearing houses
- Payments to signaling link providers
- Increased signaling traffic on own network for location updates, i.e. authentication, authorization and accounting."

"Legal and technical developments are required to remove structural barriers such as double taxation and international gateway monopolies, financial barriers such as fraud, and technological barriers such as non-harmonised technical standards. All of these are vital to reducing roaming charges in many regions." (p. 14).

The actual treaty regulating this domain is the International Telecommunications Regulations. According to the International

Telecommunications Union (ITU, the United Nations specialized agency for information and communication technologies (ICTs)), as of 21 December 2012, the total population of the countries that signed the amended 1988 treaty in 2012 was approximately 3.8 billion, comprising over 60% of the world's population. Only three countries are not party to either the 1988 treaty nor the 2012 (current) treaty. One of the major updates in the 2012 treaty includes transparency of mobile roaming prices as stated in Article 4:

ARTICLE 4

International telecommunication services

4.1 Member States shall promote the development of international telecommunication services and shall foster their availability to the public.

4.2 Member States shall endeavour to ensure that authorized operating agencies cooperate within the framework of these Regulations to provide, by agreement, a wide range of international telecommunication services which should conform, to the greatest extent practicable, to the relevant ITU-T Recommendations.

4.3 Subject to national law, Member States shall endeavour to ensure that authorized operating agencies provide and maintain, to the greatest extent practicable, a satisfactory quality of service corresponding to the relevant ITU-T Recommendations with respect to:

. access to the international network by users using terminals which are permitted to be connected to the network and which do

not cause harm to technical facilities and personnel; international telecommunication facilities and services available to users for their dedicated use;

4.4 agencies provide free-of-charge, transparent, up-to-date and accurate information to end users on international telecommunication services, including international roaming prices and the associated relevant conditions, in a timely manner.

4.5 Member States shall foster measures to ensure that telecommunication services in international roaming of satisfactory quality are provided to visiting users.

4.6 Member States should foster cooperation among authorized operating agencies in order to avoid and mitigate inadvertent roaming charges in border zones.

4.7 Member States shall endeavour to promote competition in the provision of international roaming services and are encouraged to develop policies that foster competitive roaming prices for the benefit of end users.

As with all regulations, there are challenges and even unintended consequences. The GSM Association acknowledged the following in its 2012 Information Paper: "Regulators within different regions around the world share a common concern about the level of roaming charges and customer bill-shock. However, this common concern does not translate to one global solution. This is

because only some countries have higher roaming charges, and the reasons for the higher roaming charges are likely to differ due to the different market conditions, between those countries, that have been discussed above. It follows that regulators should address their concerns at the national level in order to identify their own distinctive reasons.

A uniform, global regulatory measure may fail to address the source of any problem, and is likely to be detrimental to market performance. A uniform, global regulatory measure cannot take in account all of the different local market conditions, and thus it may fail to address the actual cause of any problem within a region. In addition, the imposition of such a recommendation may introduce new problems which harm consumers and the industry." (p. 24)

When seeking a solution to address these issues, in order to lower roaming prices ultimately requires empowering consumers, offering market based solutions and making appropriate regulatory interventions. Blocfone addresses empowering consumers and offering market based solutions globally with real time localization for national configuration capability, which in term minimizes the need for more stringent or detailed global regulatory interventions.

Blocfone™ Empowering Consumers and Enabling Providers

Imagine you are carrying your favorite mobile device, and the device is 'unlocked' or 'world ready' (this will eventually be the default, and already is for

some markets outside of the U.S.). You are traveling from your home in Atlanta to Paris on vacation, with a two day stop in NY for business in between. You rely on your mobile device for everything from email, personal and business calls, texting, reading news, playing games including video games, viewing and editing documents, accessing corporate networks, participating in video conferences for work and FaceTime with the family, watching TV and movies, the list goes on. You hate paying for and using hotel and public hotspots due to the costs, service levels, and concerns over privacy. Your mobile device includes the Blocfone app to which you have an active account setup. Your Blocfone account is associated to your Bitcoin Wallet so that you can pay for Blocfone services when needed in Bitcoin. Your Blocfone account is associated to your Atlanta 404 area code telephone number.

Since you live in Atlanta, you have selected a Blocfone offer that includes 'all you can consume 5G' voice, data and text for 10 Bitcoin (BTC) per month, available in the U.S. on any T-Mobile network. (I will use unrealistic numbers for Bitcoin to keep the math simple, as 1 Bitcoin is equal to more than $420 as of 28 March 2016, yes, prices have changed drastically since then!). You chose T-Mobile because of your typical travel patterns of visiting major U.S. cities for work several times per month rather than the countryside or small towns. You had many options when you chose the BTC 10 offer. You have no 'other offers' active at the moment.

When you arrive in NY, the mobile device automatically detects the T-Mobile network, so nothing changes, nothing happens differently, between Atlanta and NY.

However, had there been no coverage by T-Mobile in NY, and instead only Verizon coverage (simplifying, there's almost always multiple operators available in most places in the U.S.), Blocfone would recognize this gap automatically, and present many 'one click' offers to select on the Verizon network. You could select a 48 hour 'all you can consume 5G' offer for BTC 1.50 in NYC only for example. Note that I did not mention 'home network' or 'visiting network'. You are simply a customer on 'a network' under the Blocfone platform. T-Mobile is simply your 'default network' because you live in Atlanta and selected this plan to be your default in the mobile device settings. There is no more need to discuss 'contract plan' or 'no contract plan', you are simply utilizing your mobile device to select and buy offers as needed.

Two days later you land at Charles de Gaulle airport and turn on your mobile device. Again, recognizing only non-T-Mobile networks, the Blocfone app presents a number of offers, and because you do not want anything to change from a service perspective, you choose via 'one click' a 7 day 'all you can consume 5G' offer by Orange for BTC 5.00. Notice here the user experience is simple, transparent and the use of Bitcoin eliminates all FX fees and uncertainties. You did not need to replace the device SIM card with a France telephone number, you did not require buying or leasing a 'global phone', or adding an international package at JFK before taking off. You did not need to present personal information to Orange to be its customer. And best of all, you are not a slave to T-Mobile's former pricing plans that claim to offer "global 3G data for free" when in reality it is an unbearably slow carrot on a stick

sub-contracted to Orange in France anyway, and designed to get you to 'upgrade' to acceptable levels of services at exorbitant pricing schemes to which you cannot avoid, as T-Mobile is 'in control' unless you formally open a new account in France with a France operator on a mobile device compatible in France, which may or may not be the same as the device in your pocket, and certainly force you to use a France telephone number by replacing the SIM chip while visiting. Your 404 number essentially goes 'to sleep' in your suitcase unless you are tech savvy enough to implement a host of arduous workarounds such as Google Voice, which also have limitations by the way.

On the operator side, Blocfone simply presents a open platform to make offers direct to potential customers, and to provide those services based on the specific details embedded in the offers, without the need for any direct interaction with the customer other than delivering voice, data and text capability to a registered mobile device registered on its network. Blocfone, as a platform, handles the customer, distributes the offers, engages the transactions, ensures performance, and makes payments and refunds, it even includes local marketplace offers to help you during your stay.

The discussion regarding features and functions of Blocfone can go on and on, I will outline only a few others to make points of additional value. Referring back to the example, the 'all you can consume U.S. 5G' is just one of many options, a default can be Metro Atlanta only at an even lower price. The 'all you can consume'

can be limited to your true patterns 'a la carte' set as default. As Bitcoin and any cryptocurrency can be exchanged in decimal places, plans could include auto-refunds for voice, data and text that go unused in any plan period. As the GSM Association indicates, tariff innovation is the key. Blocfone pushes the envelope to bring this innovation in real time to consumers in a transparent and neutral way. An offer today can expire tomorrow, be limited in number, and any and all details such as price, features, terms and conditions, can all be refreshed and tracked securely per offer in real time.

Blocfone™ Making it Work

Centralised Counterparty

Similar to a derivatives marketplace, a centralised counterparty (in this invention a sidechain) should be implemented. This allows competing operators to deliver offers to a neutral platform and to provide the necessary trust to manage the exchange of data and money in a secure and unified manner. Operators are already adept at this concept as information and consideration is shared among home and visiting networks via a counterparty already. The difference is this counterparty brings together the consumer and provider directly. By creating an open platform in this manner, operators can continue to market products as they wish to local customers, on contract and to visitors who do not use Blocfone via home network

agreements. Nothing stops operators from continuing with 'old style' contracts and plans. On the flipside, nothing stops the consumer from giving up his/her 'old style' contract and utilizing Blocfone, even if the customer never leaves the local operator's home network. The counterparty also provides the 'ownership' of the contractual obligations to the Blocfone platform in order to facilitate the end to end process from both a customer and operator point of view.

Blockchain for Selling Voice, Data and Text

When referring to the generic term blockchain in this context, I am referring to utilizing a decentralized public ledger platform combined with mass adoption of a single cryptocurrency that provides the best possible and most secure and trusted exchange of value system. Therefore, I am referring to the Bitcoin blockchain as the method of payment to be adopted by Blocfone, although as stated earlier this is exemplary in today's view but I predict the use of branded cryptocurrencies emerging, for my BlocFone invention, this is FoneCoin, but for this paper will continue to keep it as Bitcoin. Utilising Bitcoin as the exclusive payment wallet helps eliminate concerns over fraud, data protection, know your customer, and perhaps most importantly unifies the experience from and offer perspective on the part of the operators' design and from the customers' perspective allowing apples with apples comparisons to offers around the globe. Furthermore, with the unique and permanent transaction identifier(s), and the ability to exchange Bitcoin at

micro-level decimal places, the applicability to selling data bits, voice seconds, and text characters can not be understated particularly when tracking and billing against 'usage based' offers with refunds against unused but prepaid services.

Smart Contracts of the Counterparty Associated to the Bitcoin Transaction

All provider offerings will be associated to many data elements such as price, quantity, location, time, expiration as well as a full set of terms and conditions based on the operator commitments. Taken as a whole these data elements make up the offer. All offers are unique technically, and when an offer is accepted and paid by Bitcoin, these details become permanently associated to the relevant blockchain transaction that is forever embedded in the decentralized public ledger. Upon 'loading' offers to Blocfone, the Blocfone as counterparty takes on these attributes as is its own and then exposes these details to the general public via the Blocfone app.

Sidechains for Smart Contract Templates and Oracles for Performance Management and FX

As stated earlier in the paper, the Bitcoin blockchain is already in production and contains a significant amount of useful functionality, including the basics for attaching smart contracts directly to transactions. I am asserting that the Bitcoin blockchain does not go 'far enough', and in order to enable operators to deliver

orders with associated features, terms and conditions in real time, and per offer, requires a private centralized ledger system that is unique to the Blocfone platform and utilized by the 800+ operators around the globe. This is exemplified already by Etherium, and many new entrants to the market since, and the basis of my inventions' combined BlocFone and FoneCoin standards. Additionally, while Bitcoin may be the most highly adopted cryptocurrency at the current time, operators and consumers still sell and buy in regulated local currencies. A sidechain provides the foundation to manage the FX apart from the Blocfone transaction itself, as well as branding opportunites to develop market penetration and value-add services including local marketplaces accepting single cryptocurrencies at the best deals and incentives.

Further, as templates for the smart contracts on the sidechain are developed, oracles can be developed to monitor performance and trigger actions when performance milestones are met. For examples oracles monitor offers and acceptances. Upon acceptance, oracles deliver acceptances and validation of payments to operators including transaction details and mobile device identifiers indicating the lifecycle of the activation of service through deactivation of service.

The sidechain approach works well under these conditions because the oracles can be developed and maintained based on a controlled technology platform and based on a standard lexicon. The trust of the sidechain and the oracles can utilize a similar proof of work concept as Bitcoin or any public blockchain, but be

limited to the 800+ operators. There is no incentive to hide this information or to tamper with the platform by any operator, as all of the details are open via the Blocfone app anyway. In fact, it is the opposite, as tariff innovation is the key to acquiring new customers, analytics can be achieved by operators making the semi-public sidechain a value add to the operators. From the customer point of view, these analytics can be expected to lead to better pricing and more relevant service options, enabling Blocfone to help make the overall ecosystem more efficient.

Legal Analysis for Blocfone

It is important to note two significant challenges for this legal analysis: 1) there is almost no legal content in existence today to reference beyond speculation and nascent drafts of language surrounding the still misunderstood Bitcoin and blockchain transactions in general, and there are pilot programs sponsored by major financial institutions and start-ups that offer white papers and ideas not much more descriptive than this paper; and 2) in any case I believe the Blocfone invention does not apply to most of the nascent and general blockchain regulation and laws as a result of Blocfone's very design. Instead Blocfone fits more closely to the legal issues faced by a typical CCP framework which are known, and, while I reference blockchain technology and Bitcoin as exemplary in the context of this invention, my prediction of branded cryptocurrencies such as the suggested Fonecoin™ concept would be more in line with laws and regulation that mirror programs such as

American Express Rewards Program where points are redeemable at a number of participating retailers. In this case Fonecoin would be 'redeemable' at all participating operators against offers utilizing a single cryptocurrency, with the difference being that Fonecoin actually represents the value of currencies being transferred via the network process. Essentially, in a private sidechain utilizing blockchain frameworks and accepting both existing currencies backed by assets and pure cryptocurrencies such as Bitcoin, these 'internal private cryptocurrencies' such as Fonecoin mirror the value, assets and liabilities associated to a customer rewards program, for example, in return for x miles a customer receives a plane ticket. In return for x Fonecoin, a customer receives 10gb of data in South Africa. This is the most significant departure of my innovative design with Blocfone vs. the current market fascination attempting to apply blockchain technology to the financial industry exchanging 'paper value' with no real product or service to back it up. Blocfone attempts to utilize the best of blockchain's trustless system design combined with customer-centric and disruptive approach to aggregate technically 800+ competing operators around the globe in a transparent, efficient and trusted platform that incentivizes operator participation, offer innovation customer engagement and the seamless exchange of money worldwide in return for voice, text and data services.

Nevertheless, the best paper I could find that summarizes the current state of blockchain issues the best is from a 2016 graduate of Duke University Law School,

Trevor I. Kiviat, who writes in his note paper entitled BEYOND BITCOIN: ISSUES IN REGULATING BLOCKCHAIN TRANSACTIONS the following: "No comprehensive federal regulation exists for virtual currencies. Many government bodies—specifically, FinCEN, the Internal Revenue Service (IRS), SEC, CFTC, and Consumer Financial Protection Bureau (CFPB)—have offered guidance and taken limited action."

All that said, during the course of my research I found much commentary regarding CCPs including novation, open offer, common benefits, pros and cons, risks, etc. but one paper stood out from the rest as encompassing the vast majority of what I believe are the most relevant legal issues related to Blocfone, including proposals around the use of a CCP at the center of the Blocfone invention. Therefore, I will reference the study verbatim below and utilize ***bold/italics*** to weave in my analysis throughout the quoted legal framework to indicate where I have changed or added content that applies specifically to my personal views relevant to the Blocfone invention including blockchain technology. The reference sited is from the Committee on Payment and Settlement Systems, Technical Committee of the International Organization of Securities Commissions, Recommendations for Central Counterparties, Consultative Report, March 2004 as follows:

3.11 Legal risk is the risk that a party suffers a loss because laws or regulations do not support the rules and contracts of a CCP or the property rights and other interests associated with a CCP. CCPs face a variety of such risks that have

the potential to substantially increase losses from default. Perhaps most significant is the risk that bankruptcy administrators might challenge a CCP's right to close out or transfer positions and liquidate a defaulting participant's assets. In a cross-border context, particularly that of links between CCPs, evaluation of legal risk becomes more complicated because the laws of more than one jurisdiction apply or can potentially apply to a contract. A CCP may face losses resulting from the application of a different law than it had expected. Legal risk may thus amplify the risks a CCP typically manages.

Approaches to risk management

Counterparty credit and liquidity risks

3.12 CCPs have a range of tools that can be used to manage the risks to which they are exposed, and the tools that an individual CCP uses will depend upon the nature of its obligations. Nonetheless, there are a common set of procedures that are implemented by many CCPs to manage counterparty credit and liquidity risks. Broadly, these procedures enable CCPs to manage their risks by limiting the likelihood of defaults, by limiting the potential losses and liquidity pressures if a default should occur, and by ensuring that there are adequate resources to cover losses and meet payment obligations on schedule. In designing their risk management procedures, CCPs generally seek to create incentives for participants to manage their risks prudently in the first instance.

With regard to Blocfone, the particpants would be the 800+ operators and billions of customers worldwide. The incentives would be a combination of secure payment methods in any currency and/or a single or selected cryptocurrencies, 'proof of work' standard operating procedures and oracles monitoring performance of smart contracts and triggering actions, including delivery or discontinuation of services as well as monetary transfer discussed later in the paper.

Consultative Report on Recommendations for CCPs 7

3.13 Participation requirements. The most basic means of controlling counterparty credit and liquidity risks is to deal only with creditworthy counterparties. CCPs typically seek to reduce the likelihood of a participant's default by establishing rigorous financial standards for participation. Most commonly, participants are required to meet minimum capital requirements both for admission and for continuing participation. These capital requirements are often related to the riskiness or scope of a participant's activities. Some CCPs limit participation to supervised firms; others establish a minimum acceptable credit rating. CCPs

generally do not impose specific liquidity requirements for participation, but some CCPs review participants' access to funding, especially their lines of credit from banks.

3.14 Because values of participants' positions can change quickly, CCPs often have reporting and surveillance programmes. These programmes supplement a CCP's knowledge about participants from regulatory reporting systems when CCPs have access to this information, and provide an essential source of information about non-regulated participants when regulatory information is not available. CCPs generally require participants to provide notice of any marked deterioration in financial condition, and in that event, a CCP may initiate heightened surveillance of the participant's activities and possibly impose restrictions on its dealings.

With regard to Blocfone, creditworthiness is mainly attached to the billions of customers and is inherently built-in to the payment methods, for example, using a USD Visa Debit card to purchase Bitcoin from a standard Bitcoin management platform (e.g. Coinbase) to finally be used to purchase voice, text and data in Fonecoin in England based on a specific global Blocfone unexpired offer registered on the trusted Blocfone private blockchain ledger and displayed on the Blocfone App. The offers of voice, data and text are essentially the asset being exchanged for consideration, in small and controllable amounts (i.e., for a day, a week, a month). Since the asset itself is by form electronic, it is forever controlled by the 'asset custodian' operators and can be activated (delivered, transferred) and deactivated (un-delivered, transferred back) instantaneously via a trigger from an oracle should the financial transaction be reported back to the Blocfone CCP as pass or fail. If a 'pure cryptocurrency' (e.g. Bitcoin) is embedded within the transaction, it is the Bitcoin blockchain network itself covered by the legal and regulatory issues surrounding a 'pure cryptocurrency', and Blocfone as a platform is merely a beneficiary of the inherent risks of accepting Bitcoin as a merchant.

3.15 In addition to financial requirements, some CCPs establish standards of operational reliability that address a participant's ability to submit deal-related information ***and services, in this case the operators providing voice, text and data*** in a timely fashion and to continue operations even if a participant's primary operating system is disrupted.

3.16 Collateral requirements. Participation requirements cannot reasonably be expected to eliminate the possibility of default, and thus CCPs require participants to post collateral with the aim of limiting the CCP's losses and liquidity pressures in the event that default occurs. A CCP typically imposes requirements that participants provide collateral (or guarantees) to cover potential future losses

on open positions. These requirements are often set to cover some high percentage of likely price movements (say 95-99%). CCPs for derivatives transactions generally refer to these requirements as margin requirements.2 A few CCPs refer to the collateral posted to cover potential future losses as a guarantee fund or clearing fund. This latter terminology for the collateral posted is more commonly employed by CCPs for cash markets. Regardless of the terminology, the common risk management tool is a requirement to post collateral that serves to protect a CCP against some high percentage of potential future losses on its contracts with its participants. In this report, we refer to such requirements as collateral requirements.

3.17 The effectiveness of collateral requirements depends on a CCP's ability to measure and manage the build-up of exposures. CCPs regularly mark contracts to market and measure the exposures that have arisen as a result of price changes since the last valuation. They generally require participants to cover these current exposures in one of two ways. Some CCPs require participants to pay cash equal to the amount of losses to the CCP; these cash payments are passed to participants whose positions have gained in value. Other CCPs require participants to post collateral to cover mark-to-market losses. (In this latter methodology, participants whose positions have gained in value do not receive explicit payments; rather their holdings are now over-collateralised, and the excess collateral can be withdrawn.) These types of payments are often referred to as variation margin payments. Regardless of the method used by a CCP, the effect either of the cash payment or of the collateral posting is to eliminate the current exposure on the position.

Essentially, for Blocfone, the collateral can be nothing more than a promise in a contract by enhancing the existing contracts operators have among themselves in the current environment allowing for customers to roam and including transfer of value and payments. Yet in this instance, these agreements are the fallback position, if and only if a failure occurs in providing services to customers directly via the Blocfone App. The customer benefits by the seamless experience, and the operators benefit because they already have recourse available automatically should their operations structure fail (e.g., an Offer accepted by a customer of Operator 1 fails to be delivered by Operator 1 but can be delivered by Operator 2 is automatically transferred (novation) to Operator 2 per agreement between Operator 1 and Operator 2, and value is then transferred from Operator 1 to Operator 2 'behind the curtain' at no additional cost or detriment to the customer. Customers require no collateral as the operators are in full control over the delivery (or rescinding) of the asset. Instead, losses for customers are mitigated by contractual obligations of the operators providing services, and the losses for operators are mitigated by the small nature of each transaction combined with the control of discontinuing

services instantaneously. As no transaction can have 100% certainty, there will always be some 'acceptable' risk of loss on both sides of the equation handled in different ways (e.g., a write-off on the operator side, a disputed credit card charge on the customer side).

3.18 The key determinants of the protection against credit losses provided by any type of collateral system are: (1) the procedures used to determine the level of collateral required, including the percentage of potential losses that a CCP intends to cover and the methodology it uses to estimate potential losses; (2) the frequency of updating position information; (3) the frequency of marking positions to market, collecting collateral and cash payments and eliminating current exposures; and (4) the price stability and liquidity of the assets accepted as collateral.

3.19 Financial resources. The collateral system is but one component in the package of techniques available to a CCP to mitigate credit and liquidity risks. While collateral requirements provide substantial protection to a CCP, losses in the event of a participant's default might exceed the collateral posted for several reasons. Collateral requirements cover a high percentage of likely price movements, but they are not set at a level that is intended to cover all price movements. More time might elapse before a CCP could liquidate a defaulting participant's positions (for instance because of illiquid markets) than was assumed in setting the requirement. Furthermore, a defaulting participant may have increased its positions since the last settlement. CCPs thus maintain resources to cover their uncollateralised losses and to provide liquidity while realising the proceeds of a defaulting participant's assets. These resources, together with the collateral system and risk management tools such as participation requirements, determine the overall level of protection provided by the system and how risks and costs are shared among the stakeholders of a CCP.

3.20 For the purposes of this discussion, collateral requirements will refer to those requirements set to cover a large proportion of a CCP's likely exposures to its participants. Other financial resources that a CCP holds, by contrast, are recognition that market conditions may occur that fall outside the bounds of exposures a CCP normally seeks to cover, and thus a CCP needs additional resources for these contingencies. Some CCPs hold a single blended pool of resources that is intended to cover both a large proportion of likely exposures and exposures resulting from more unusual market conditions.

3.21 Many CCPs use stress tests to assess the adequacy and liquidity of their financial resources. In these tests, a CCP assumes price moves substantially larger than those the collateral requirements are designed to cover. It examines the magnitude of uncollateralised exposures that result from such price moves and

assesses whether a CCP's resources would be large enough to cover exposures from one or more defaults.

3.22 Financial resources can take the form either of assets held directly by a CCP or of contingent claims. Resources commonly held directly include a CCP's capital, reserves and clearing funds. The latter are collateral pools provided by participants for a CCP's use in the event of default by any participant. Some CCPs have contingent claims on participants' resources. For example, a CCP may have the authority to assess non-defaulting participants to cover losses. Other contingent claims include a guarantee provided by a parent organisation (either of the CCP itself or of participants) or a default insurance contract. The balance between resources held directly versus those that represent contingent claims varies greatly from one CCP to another.

3.23 The liquidity of financial resources and the manner in which they are held is also of issue because CCPs generally commit that their obligations will be met without delay. But many of a CCP's resources cannot be mobilised within a trading day. CCPs thus obtain committed credit lines that allow borrowing against assets as part of planning for liquidity needs.

The major advantage of Blocfone here is the trustless yet private blockchain platform design combined with oracles and smart contracts to instantly detect and mitigate potential loss, so while the concept of collateral exists, it is different due to the nature and size of the transaction, the asset type exchange, control and ultimately the design of the trusted blockchain framework including sidechains, oracles and smart contracts.

3.24 Default procedures. In the event of a default, a CCP must take steps to contain and ultimately to eliminate its exposure to its defaulting participant. The longer the positions carried by a defaulting participant remain open, the larger are the potential credit exposures on those positions. A CCP's primary safeguard in this event is the ability to transfer, close out or hedge positions of a defaulting participant quickly. In this regard, a CCP might be constrained by the size of a defaulting participant's positions and the liquidity of the markets in which they were held. If a participant is also carrying positions for customers, those positions are typically transferred to a non-defaulting participant, or in some instances the customer positions also are closed out.

3.25 The rules of CCPs specify the order in which resources will be used in the event of a default. To create proper incentives for participants to manage their own exposures, the first resources tapped are those of a defaulting participant - the collateral it has posted with a CCP and any other assets that a CCP might have a

claim on. If a defaulter's resources are insufficient to cover a CCP's losses, a CCP will turn to its own resources or those of non-defaulting participants. How these latter resources are tapped varies widely, with some CCPs first seeking resources from participants that dealt with a defaulter and others mutualising losses. (The rules of some CCPs also specify different resource pools for defaults occurring in different products.)

Here the rules would play out well on the Blocfone CCP if designed with appropriate risk distribution parameters among operators, customers and CCP. I would argue the efficiency and benefits stem from Blocfone's real-time assessment of each and every transaction (ledger entry via proof of work process and smart contract triggers) to create and maintain an efficient market with low waste (i.e., loss) to all parties.

Settlement bank risk

3.26 Some CCPs eliminate the risk of settlement bank failure by using the central bank of issue as the sole settlement bank. If the central bank is not used, a CCP typically manages the credit and liquidity risks arising from the failure of a settlement bank through choice of the settlement bank or banks and contractual arrangements that minimise the amounts and durations of its exposures to those banks.

In this regard, Blocfone would utilize a single, global settlement bank with a robust global transaction banking platform (e.g., Deutsche Bank). As Blocfone is a platform to offer and purchase voice, text, and data services, there is no competitive conflict of interests among participant operators, rather efficiency, simplicity, reliability, and transaction fees are priority.

Custody risk

3.27 By carefully selecting custodians and monitoring the quality of accounting and safekeeping services provided by those custodians, CCPs seek to limit custody risk. A key concern is that the custodian's procedures protect a CCP's collateral against the claims of the custodian's creditors. A CCP typically requires that custodians demonstrate strong internal controls and an ability to move collateral promptly in accordance with legitimate instructions from it.

Investment risk

3.28 CCPs face credit, market and liquidity risks from investing their own financial resources and from investing cash collateral posted by participants. To

limit these risks, investments may be secured. CCPs usually establish standards for the creditworthiness of obligors and limit investment to relatively liquid instruments. Limits on concentrations of investments by obligor may also be utilised.

Operational risk

3.29 CCPs face a variety of operational risks related to the functioning of both personnel and systems. Typical safeguards include programmes to ensure adequate expertise, training and supervision of personnel as well as establishing and regularly reviewing internal control procedures. Operational safeguards for CCPs also address both the availability and the capacity of a CCP's computer systems, communications systems, power sources and data feeds. Fundamental is a CCP's business continuity plan that addresses events posing a significant risk of disrupting operations and enables a CCP to continue to meet its obligations on time.

Legal risk

3.30 CCPs manage legal risk through a well founded legal framework that supports each aspect of a CCP's operations and through careful review of relevant law and design of contracts and rules, both at creation and on an ongoing basis. Depending upon the legal structure of the jurisdiction where a CCP is established, legislation specific to a CCP may be the most effective means of ensuring it has a well founded legal basis. Some jurisdictions, for example, have special legislation addressing netting or a CCP's ability to take actions in the event of a participant's default. Other tools for mitigating legal risk are careful drafting of a CCP's rule book and contracts to ensure that the obligations of a CCP, its counterparties and agents are clear and that laws of relevant jurisdictions support the application of its rules.

Blocfone as a platform would include a standard operator and customer agreement localized only to accommodate local statutory, regulatory or legal demand. There would be no cherry picking power among any operator or customer.

3.31 As cross-border participation and product offerings of CCPs have grown, along with links between CCPs, the need for legal analysis in multiple jurisdictions has also grown. In some instances, CCPs can choose the law intended to apply to parts of their operations. In other instances, a conflict of laws may exist. CCPs manage such legal risk in the first instance through adaptations to their rules and contracts. For example, if a CCP is unsure that its rules may be upheld in another jurisdiction, it may require participants from that jurisdiction to hold more collateral or to hold collateral only in the CCP's own jurisdiction.

The key element for Blocfone to be a success is to have an oracle that governs a clear process beginning with a default, single jurisdiction selected for mandatory arbitration (e.g., France), and to trigger alternatives based on an 'if then' set of criteria where known conflict of laws exist or to mitigate other 'localised legal quirks' to which all criteria favor operators and Blocfone as an entity in and of itself. The risk of legal action is more likely to occur among operators and Blocfone, as it is unlikely that legal action would be taken by a customer over service issues (i.e., it is cheaper to offer a refund to a complaining customer via a simple online form than to litigate, regardless of jurisdiction or fault). On the other hand, there are unusual circumstances to consider (e.g., my phone didn't work so I could not call an ambulance and the results were catastrophic) but these extremes can be covered by insurance better than an electronic oracle sorting through a jurisdiction formula to mitigate customer litigation scenarios.

10 Consultative Report on Recommendations for CCPs

4. Recommendations Recommendation 1: Legal risk

A CCP should have a well founded, transparent and enforceable legal framework for each aspect of its activities in all relevant jurisdictions.3

4.1.1 A well founded legal framework should support each aspect of a CCP's risk management and operations. The legal system (including bankruptcy laws) should clearly support: novation, netting, default procedures, collateral and clearing fund arrangements, enforceability of a CCP's rules with regard to its participants, conflict of laws determinations, and access to information. Further, the laws and regulations governing a CCP, a CCP's rules, procedures and contractual arrangements, and a CCP's timing of assuming its obligations should be clearly stated, internally coherent and accessible to participants and the public. If the legal framework is underdeveloped, opaque or inconsistent, the resulting legal risk will undermine a CCP's ability to operate effectively. Financial market participants will face the dilemma of either: (1) using a CCP with an incomplete ability to assess their risk of participation; or (2) declining to use a CCP. Under either circumstance, the risk reduction benefits of a CCP may not be realised and, depending on the significance of weaknesses in the legal framework, the activity of a CCP could be a potential source of systemic risk.

4.1.2 In most jurisdictions, the legal concept that enables a CCP to become the counterparty is either novation or open offer. Through novation, the original contract between the buyer and seller is extinguished and replaced by two new contracts, one between the CCP and the buyer and the other between the CCP and

the seller. In an open offer system, a CCP is automatically and immediately interposed in a transaction at the moment the buyer and seller agree on the terms. If all pre-agreed conditions are met, there is never a contractual relationship between the buyer and seller in an open offer system. Either novation or open offer gives market participants legal certainty that a CCP is obligated to effect settlement if the legal framework is supportive of the method used.

I would argue that Blocfone smart contracts between operators and customers begin with a standard template per jurisdiction enabling operator configuration PER OFFER. This is the hook that allows providers across borders to contract directly with customers worldwide on a standard platform, with a standard payment methodology, but with unique and innovative offers backed by its own terms and conditions that can change at any time but will never be lost once offered and accepted. This favors a novation scenario rather than open offers in order to effectuate per transaction Blocfone as a the platform of record that maintains indefinitely and independently the contract terms and conditions PER OFFER. There are caveats: 1) certain clauses would not be configurable (e.g. choice of jurisdiction, arbitration, notice procedures to name a few); 2) there would not be an infinite number of configurable offer elements in order to promote system-wide performance and efficiencies; and 3) there may be other reasons that benefit the collective participant community more than any individual. The major reason blockchain and private sidechains enhance the Blocfone offering is to provide the trust and accuracy that each and every transaction recorded on behalf of competing companies and global customers, and accepting by a transparent proof of work process can be retrieved at any time to further a cause such as defense in a legal action among other reporting and analytics concerns and aspirations.

4.1.3 The legal framework should support the essential steps that a CCP takes to handle a defaulting or insolvent participant, including closing out a participant's positions. A CCP must act quickly in the event of a participant's default, and ambiguity over the enforceability of these procedures could delay, and possibly prevent altogether, a CCP from taking actions that fulfil its obligations to non-defaulting participants or minimise its potential losses. Insolvency law should support isolating risk and retaining and applying collateral and cash payments previously paid into the CCP, notwithstanding a default or the commencement of an administration or bankruptcy proceeding by or against a participant. It is important that the legal framework provide certainty as to how the insolvency of a CCP would be handled.

Blocfone would offer participants standard performance guarantees and service level agreements at the platform level for any given time unlike the offer terms and conditions which are configurable at the offer level.

4.1.4 The legal framework must enable a CCP to clearly establish its interest in collateral. Generally, collateral arrangements involve either a pledge or a title transfer. If a CCP accepts a pledge, it must have a high degree of assurance that the pledge has been validly created in the relevant jurisdiction and validly perfected, if necessary. If a CCP relies on a title transfer, it should have a high degree of assurance that the transfer will be enforced as written and not recharacterised as a pledge (which would probably be an invalid or unperfected pledge).

This is exemplified by a blockchain, private blockchain, smart contracts and oracles based architecture !

4.1.5 A strong legal framework will support the rapid deployment of the collateral held by a CCP when a participant defaults on its obligations or becomes insolvent. This aspect of the legal framework is critical because delay in the use of collateral may prevent a CCP from meeting its obligations as expected. The legal framework will accomplish this goal if the rules and contracts for operating a CCP and the obligations of its participants are enforceable, and a CCP has the unimpeded ability to liquidate collateral and close out transactions.

Oracles.

4.1.6 The enforceability of a CCP's netting arrangements must also have a sound and transparent legal basis. Netting involves the offsetting of obligations by trading partners or participants. CCPs often bilaterally net their obligations with each participant. Netting reduces the number and value of deliveries and payments needed to settle a set of transactions and significantly reduces the potential losses to a CCP in the event of a participant's default. Some CCPs also net gains and losses from the closeout of positions in different securities or derivatives. Netting arrangements must be enforceable against a CCP's failed participants in bankruptcy. The legal framework should support the CCP's netting arrangements. Without such legal underpinnings, net obligations may be challenged in judicial or administrative insolvency proceedings. If these challenges are successful, the CCP or its participants would be obligated for gross amounts - potentially a huge, even devastating, change because the gross obligations could be many multiples of the net obligations.

The benefit of a netting arrangement can also be leveraged within oracles to determine the best route so that the cost of transferring currency values across borders minimizes transaction fees

4.1.7 A critical issue in a CCP's money settlement arrangements is the timing of the finality of funds transfers between the CCP's accounts and the accounts of its participants at the banks used to effect such settlements. The funds transfers should be final, ie irrevocable and unconditional, when effected, that is, when accounts are debited and credited. The laws of the relevant jurisdictions must support the provisions of the CCP's legal agreements with its settlement banks relating to finality.

4.1.8 Where a CCP crosses borders through linkages, remote participants or the taking of collateral, the rules governing the CCP should clearly indicate the law that is intended to apply to each aspect of the CCP's operations. Potential conflict of laws should be identified and the CCP must address conflict of laws issues when there is a difference in the substantive laws of the jurisdictions that have potential interests in a CCP's activities. In such circumstances, each jurisdiction's conflict of laws rules should specify the criteria that determine the law applicable to the activity. CCPs should take into account the conflict of laws issues when structuring their rules and choosing the law that governs the CCPs. Both CCPs and participants also should be aware of applicable constraints on their ability to choose the law that will govern a CCP. A jurisdiction ordinarily does not permit CCPs and participants to circumvent the fundamental public policy of that jurisdiction by contract.

4.1.9 In some markets, trade guarantees are not provided by a CCP but through an alternative arrangement that does not involve either novation or closing out a participant's positions. The most common arrangement is when the stock exchange or other entity (a guarantor) has established a default or guarantee fund to "guarantee" all trades between market participants. Generally, a guarantor is not a counterparty and, therefore, is not obligated to fulfil the settlement obligations of a defaulting participant. Rather, a guarantor undertakes to indemnify its participants against losses incurred when they close out and replace contracts with a defaulting participant. The legal framework should provide a high degree of assurance that rules and procedures are enforceable by the guarantor. A well founded legal framework should also support a guarantor's obligations to non-defaulting participants and the guarantor's procedures for using the fund's assets. These procedures should be transparent and consistent.

4.1.10 A CCP or a guarantor and the appropriate regulatory authorities should organise and license a CCP or guarantee fund in a manner that enables it to take advantage of all of the legal protections available in the jurisdiction. Regardless of its organisation or regulatory status, a CCP or a guarantor should have the legal authority to establish requirements for direct access to its services and deny access to entities that fail those requirements. Further, legal, regulatory or confidentiality

restrictions should not prevent market participants from providing information about themselves germane to their participation in a CCP or guarantee fund.

Key issues

1. The laws and regulations governing the operation of a CCP and a CCP's rules, procedures and contractual provisions for its participants should be clearly stated, internally coherent and accessible to participants and the public ***via the Blocfone App***.

2. The legal framework should provide a high degree of assurance for each aspect of a CCP's operations and risk management procedures.

3. The rules, procedures and contracts of a CCP should be enforceable when a CCP participant defaults or becomes insolvent.

4. A CCP should identify and address any potential conflict of laws issues arising from cross- border arrangements.

Key questions

1. Are the laws and regulations governing the operation of a CCP and the rules, procedures and contractual provisions for its participants clearly stated, internally coherent and accessible to participants and the public?

2. Does the legal framework demonstrate a high degree of assurance that there is a clear and effective legal basis for:

- The CCP to act as counterparty.
- The timing of assumption of liability as CCP or guarantor trade guarantee.
- Netting arrangements.
- The CCP's interest in collateral that a participant pledges or transfers to the CCP and that this interest cannot be defeated by the participant or a third party.
- Default procedures.
- Finality of funds transfer.
- Other significant aspects of the CCP's operations and risk management procedures.

3. Are the rules, procedures and contracts of the CCP enforceable when a CCP participant defaults or becomes insolvent, notwithstanding the particular provisions of the insolvency laws?

4. Is there a significant level of cross-border participation in the CCP? Has the CCP determined whether there are other jurisdictions relevant for determining the adequacy of the legal framework? Has the legal framework been evaluated for the other relevant jurisdictions? Do laws and rules support the design of any cross-border arrangement and provide adequate protection to both CCPs in the operation of the arrangement? Are there conflict of laws issues and, if so, have they been addressed? Have cross-border collateral arrangements been evaluated?

1. In addition to supporting the core CCP activities discussed in this section, a well developed legal framework should have a well defined system of property, contract, securities, trust, bankruptcy and tax laws. Also, the legal framework must permit relatively speedy access to the court (and, if applicable, arbitration) systems, must produce final judgments, and must provide a relatively convenient mechanism to enforce judgments.

2. In assessing legal risk, the phrase “high degree of assurance” is used frequently. This is because statutes and rules are often untested in court, and so CCPs and participants rely on opinions of legal counsel as to the likely outcome of possible challenges to the scope and enforceability of such provisions.