GamCrowd®

CHAIN FINANCE

“What will be the impact of blockchain on the gambling industry?”

13th July 2017 2nd Edition

Foreword

Mark Blandford

iGaming Entrepreneur and Blockchain Investor

“Along with many others, I think I made the mistake a few years back of thinking that Bitcoin was ‘just’ a virtual currency – but when I started to dig deeper, I came to understand that what is truly disruptive about cryptocurrencies is the technology that underpins it.

This is why this report from GamCrowd is so timely and important. Blockchain technology has the potential to affect a huge array of areas in our lives. In particular, I believe the financial landscape will be transformed by blockchain.

And so, potentially, will the gambling industry. Already we are seeing entrepreneurs and others marching ahead into areas such as betting exchanges and provably fair games (see the report for more detail here), but I know there is more to come. We know that blockchain has the potential to revolutionize the banking industries due to significant cost reduction, compliance and simplifying back office operations. The same goes for the gambling sector.

I think Bitcoin originally was adopted by libertarians who saw it as a revolutionary way of making payments without ‘Big Brother’ watching them. In actual fact, I think this unique technology with the unique identifier code is going to do great things in terms of anti-money laundering where everything is going to be auditable and traceable in a far more transparent way.

I have said before that I believe the online gaming industry should be very interested in blockchain and its ramifications. This report is a fantastic start, giving a primer on how blockchain has developed and I can only but applaud GamCrowd for putting it together at this time.

If you aren’t reading this report and digesting it, no matter what area of the gambling industry you work in, then I suggest that you are in danger of missing out”

TABLE OF CONTENTS

I. Glossary of Blockchain Terminology

Glossary of Terms

Bitcoin - an electronic cash system and first cryptocurrency launched by Satoshi Nakamato as open source software in 2009. Without any trusted central authority, bitcoin utilizes a distributed ledger based network of communicating nodes running bitcoin software that records bitcoin transactions and maintains the network. The bitcoin cryptocurrency is most often abbreviated as BTC.

Blockchain - a distributed database or ledger spread over a network of computers or devices that maintains a growing amount of records secured from tampering and revision, which each block of data in the chain containing a timestamp and a link to a previous block.

Cryptocurrency - A medium of exchange or digital currency that is secured, transferred and generated through applications of cryptographic technology. Cryptocurrencies are often called crypto or digital tokens or coins.

DAO - decentralised autonomous organization is an organization that is run through rules encoded in smart contracts. The financial transaction record and program rules are maintained on a blockchain.

DApp - distributed application is a software application that utilizes a blockchain and its features to enhance the types of legacy software services traditionally provided in centralized network systems or provide innovative applications altogether.

DLT - distributed ledger technology - synonymous with blockchain technology.

Ether - (also ETC) Ethereum blockchain's native cryptocurrency.

Ethereum - a next-generation blockchain / distributed ledger platform designed for provision of smart contract technology and a multitude of decentralized applications.

Hash - A hash algorithm transforms an arbitrarily-large amount of data into a fixed-length hash. This hash will always be generated from the same data, but modifying the data even slightly will completely change the hash.

ICO - an initial coin offering is usually a crowdsale of a proprietary cryptocurrency (token or coin) for the purpose of raising funds. The native coin may also have a function in a particular distributed application or platform.

Nonce - In cryptography, a nonce is an arbitrary number or bit string that may only be used once. In online gambling, cryptographic nonces are used with server hash and user browser hash to generate a provably fair random number.

Node - any device, computer or server that connects to a blockchain network is called a node. Nodes fully enforcing all rules of a blockchain are called full nodes and form the backbone of the network.

Oracles - Oracles are software, hardware and human agents that illuminate and authenticate real world events and submit this data to the distributed ledger for use in smart contracts and resolving disputes.

Permissioned Ledger - blockchains or ledgers that are private and require members to have permission from the other members or an authority to be participants.

Permissionless Ledger- blockchains like bitcoin that are public and require no permission to join the network. They will however require hardware of minimal specifications, and need to be connected to the Internet as well as have the ability to download the blockchain on to the device.

Proof-of-Stake -Proof-of-Stake (often PoS) is a blockchain consensus mechanism that is considered more environmentally friendly than Bitcoin's Proof-of-Work, which needs significant raw computing power to generate hashes. The PoSmethod is concerned with the just the validation of blocks rather than the actual mining of new blocks, and demands that the node shows ownership of a certain amount of currency. The more of a currency there is, the more validating power the node gains.

Proof-of-Work - Proof-of-Work (often PoW) is an algorithm for reaching consensus on the blockchain that requires users to perform a degree of work to participate. In bitcoin, participants use powerful servers or computers solve difficult mathematical problems - described as certain amount of brute force work - and eventually find or mine bitcoin.

Provably Fair - a tool or algorithm in online gambling that enables a player to verify fairness on the part of the service operator.

SHA256 - a hash algorithm used by the bitcoin blockchain to generate verifiably random numbers with a predictable amount of CPU effort. Generating a SHA-256 hash with a value less than the current target solves a block and mines some bitcoin.

Smart Contracts - pre-written software code that is stored and executed on a blockchain, carrying out functions when pre-set conditions are met. smart contracts are self-executing as written, can control and disburse assets, and cannot be interfered with.

Trustless - in distributed ledger technology, trustaless describes a system where there is no need for a trusted third-party.

Wallets - Cryptocurrency wallets can be software-based or hardware-based, hot or cold. A "Hot Wallet" is any wallet that connected to a network or to the Internet. A "Cold Wallet" is one that is offline. A software wallet is a software application that holds cryptocurrency, and a hardware wallet is a hardware device that stores cryptocurrency.

Sidechain - Process used to move cryptocurrencies from one blockchain to another.

Off chain - A process not taking place on the blockchain.

II.

INTRODUCTION

Origins of the GamCrowd Blockchain Report

Welcome to the second edition of our popular report that sets out to explain what the blockchain is and to look at the developing landscape for this truly transformational tech and the potential impact on the gambling industry. The speed of progress since we first published the report in November last year has proved that the pace of change with new tech trends is like nothing we have experienced before. If you don't understand what is happening, then you are putting your business at risk it is simple as that. The fact that you are reading our report shows you have made the first step and the report will help you to start to work out how you can exploit the tech and in equal measure prepare for the disruption that it will bring.

One key development our report covers is that there have been several successful Initial Coin offerings or ICO's by various start-up gambling businesses using the blockchain to bring platforms that could bring major disruption to the way the industry operates now. Not only are they using the blockchain to try and give players a better experience, they are also very well-funded with over US$50 million being raised in the past six months alone. The gambling industry has never seen well- funded start-ups that don't have to rely on the major operators for a leg up to help them launch their business. They are in control of their own destinies and armed with disruptive tech so the gambling industry should sit up and pay attention!

One of those is funfair.io who raised $26 million in four hours! These guys have built a business around the provably fair properties of blockchain where they can prove the RNG is trustless and that they don't operate a wallet system where the player is in control of their own funds at all times. On top of that they get paid straight away after each win! If this works what player in their right mind would play with any of the existing operators where they hold on to your money as long as they feel fit to pay you out!!

Of course, you must bring a level of cynicism to what is happening as the ICO's market as it feels like the internet bubble all over again and whilst the process is unregulated the pirates out there will make money from the developing space. However, the important thing is not to confuse an ICO with the technology. To do that will be to the same mistake people made with Bitcoin with the negative press it experienced and miss the tech that is the platform that delivers these products. The biggest irony is that the gambling industry will be protected for a time by regulators slowly adopting the technology. This is despite that fact that blockchain can solve many of the regulatory processes, and the RegTech sector is one of the fastest growing areas supporting FinTech.

GamCrowd is all about innovation in technology, and there is potentially no more exciting area than blockchain. If you would like us to come in and talk to your team about the tech, then we are holding day seminars and have various packages available. If you're interested, then please email chrisnorth@gamcrowd.com for more information.

We will keep up to the latest developments so we can update this report in future.
Buckle up, blockchain is here and it's on steroids!

All the best
Chris North, CEO GamCrowd, Dr. Hans Lombardo, Chain-Finance.

III. Defining Blockchain & Distributed Ledger Technology

The blockchain first rose to prominence as the technology behind the cryptocurrency bitcoin. Since the bitcoin white paper of 2008, many different cryptocurrencies have been developed using the bitcoin blockchain and other types of blockchains. Cryptocurrencies are digital units of value created using cryptography to secure the transactions and to control the creation of additional units of the currency. Despite the original intention behind its creation, the blockchain, often described as a distributed ledger, has moved beyond being a platform for launching cryptocurrencies to being a potential platform for distributed applications in different areas and industries. Although a blockchain ledger is a record of transactions, its characteristics and strengths are above and beyond what would be associated with its traditional counterpart.

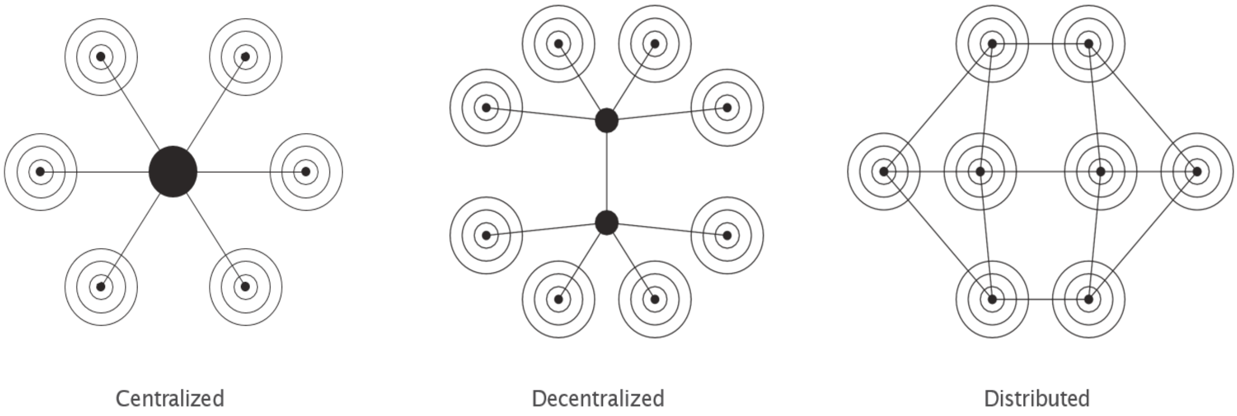
With a traditional paper ledger, bookkeepers kept a record of every company or organizational transaction in order to manage a company's monetary resources and financial health. This created a single central record of accounting to reference in order to keep the company operating and generate a company's periodic financial reporting. The advent of computers, accounting software and the Internet made it possible to create electronic versions of corporate ledgers in the form of computer databases that were easier to store, disseminate and share with managers globally. The development of network servers and Intranets meant that corporate executives could be kept informed with real-time financial information from corporate accounts. This type of network computing relies on a centralised server model where processing of transactions occurs in one place with a single point of failure, making the corporate ledger or database vulnerable to both hacking and technical failure.

The blockchain is an evolution of the network server model in that it is a distributed database structure with a secure write-forward authentication system for adding data and without a single point of failure evident in traditional database structures. With the blockchain, any full node - computer, server or device - that participates in the network gains a copy of the ledger. These blockchain devices form the points of the network and can be described as 'nodes'. Through nodes, users can update or input information into the ledger without going to a third party, giving much more power and flexibility to individual participants in the network. Each node of the distributed ledger is in communication with every other node, allowing regular updates and verification to take place. If network nodes fail in a blockchain, the network compensates for this loss as there are copies of the blockchain on the thousands of devices that are nodes. The multiple benefits of this innovative distributed network model make it ideal for implementation across a wide range of industries.

> "
> A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of 'keys' and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network. "
>
> - "Distributed Ledger Technology: beyond block-chain", A report by the UK Government Chief Scientific Adviser[1]

Figure 1: Database Structures

(dark circles represent controlling servers and points of failure)



Key Features

The various blockchain protocols can have different characteristics and strengths. However, those blockchains normally share these innovative features:

- Immutable (permanent) records
- Highly secure
- Anonymity & transparency
- Removes intermediaries
- Validation and authentication engine

Immutability

One of the main selling points of any blockchain is that it is a immutable or permanent record of all transactions ever made on the network. In other words, when data is put onto the blockchain it cannot be changed by anyone for any reason at any time. When a new block of data is added to the blockchain, it is defined and linked to the previous block by a unique hexadecimal chain of numbers and letters called a hash. If any detail, no matter how small, is changed then the hash would change. As the hashes link the blocks to previous ones, a change in the hash would be instantly recognised and rejected by the rest of the network. This resulting immutability is hugely beneficial for auditing and means that data, and the time it was entered, written into the blockchain can be trusted to not change from when it is entered. What is not guaranteed, however, is that information entered on the blockchain is accurate in the first place, although there are companies working on methods to ensure verified data can be automatically uploaded.

Security

Another key characteristic that blockchain is known for is being highly secure. The reason for this is that blockchains utilize consensus protocols in the addition to the fact that every 'node' in the network has a copy of the blockchain and participates in achieving consensus. Whenever a new block of transactions and data is added to the blockchain, the details are published to the network. Each node then ensures the veracity of the new block by checking that the data it contains does not conflict with the existing data. If more than a predetermined fraction of the network (50% in the bitcoin blockchain) agrees that the data is correct, then it is published; whereas if not enough of the network verify, the data it is rejected. A hacker could only overcome the blockchain network after overcoming at least 51% of the thousands of nodes participating in the network. As there is no central authority to target, hacking a blockchain is almost insurmountable task that only gets more difficult as the network grows. Whilst hacks leading to large heists of cryptocurrency have been reported, it is weaknesses in traditional network security of wallets or exchanges that have been compromised, not the blockchain itself. Since its inception, the bitcoin blockchain has never been hacked. With the blockchain ability to rapidly replicate and without central points of failure, DDoS attacks, power outages, government intervention or any other events that shut down part of the network will be unable to stop a blockchain system functioning. So long as one part of the network is still running, the network will continue. If the attack, power loss or restriction ends, then the part that lost service will be updated when it comes back online by the rest of the network.

Anonymity

A feature of blockchains that has been a concern of authorities has been the anonymity of its network users. Within a blockchain like bitcoin, people or nodes are identified by a unique ID. In these blockchains, there is no requirement to register a person's actual identity alongside their ID. The anonymous nature of the network's users has led to some exploitation of the bitcoin blockchain for illicit or criminal activity, including utilisation for narcotic sales, money laundering, and fund raising by organised crime and terrorist groups (link to Silk Road article). Even though government assessments suggest that use of blockchain for such activities is low in volume and traditional banking is still a lot more vulnerable to "money laundering and terrorist financing"[1], the public perception of cryptocurrencies is that they are plagued by criminals.

Transparency

Ironically, it is the transparency of the blockchain that can mitigate criminal activity. In the bitcoin blockchain, the details of all data and transactions between anonymous network participants are also open and visible to all members and non-members of the network. Anyone with an Internet browser can use a blockchain explorer to gain a snapshot of the blockchain by entering a block, transaction or wallet address.[2] The virtue of transparency and its openness means that everyone has a form of censor-free platform. Given this value of transparency, it could be said that the anonymity purportedly granted by blockchain is not guaranteed. By tying a network participant's ID to their real life identity, authorities can work out an entire host of transactions by that particular individual. It also means that when cryptocurrency is used in a known illicit activity it can be traced to different parties who use it. Indeed, some financial institutions and authorities are considering using blockchain technology to combat money laundering and fraud.[3]

[1] HM Treasurey "UK national risk assessment of money laundering and terrorist financing" - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf

[2] A blockchain explorer is basically a browser of the blockchain. Examples include https://blockexplorer.com/, http://blockr.io/ and https://live.blockcypher.com/btc/.

[3] A. Woodhouse,"Blockchain technology can help banks beat money laundering" South China Morning Post, 8 June 2016, http://www.scmp.com/business/banking-finance/article/1969769/blockchain-technology-can-help-banks-beat-money-laundering

Disintermediation

The distributed model of the blockchain is purely peer-to-peer, removing intermediaries or middle parties that are common in the modern banking system, online payment platforms like Paypal or remittance networks like Western Union. This reduces the cost of operating for those on both sides of transactions, and opens up possibilities in banking and finance to massive unbanked populations in the developing world. Without the costs associated with traditional banking and remittance, particularly across borders, and the removal of central authorities from the network, the blockchain system is more open to people who wish to use it, as long as they have an Internet connection. This prevents certain sections of societies from being blocked from accessing the technology, even in countries where women are not permitted to open a bank account without permission from a man. access to a computer with internet connection they could use a blockchain to control their own finances.

Authentication and Validation

Another important capability of blockchain is in its ability to authenticate users and validate transactions. For even just using bitcoin as a e-cash system, users have a growing choice of secure wallets with multi factors of authentication. The more factors of user authentication that are employed, including passwords, email or SMS messages with codes, fingerprints or other biometrics, the greater the security of accounts, as well as software and hardware wallets. There are at least 12 startups that are leveraging the blockchain to authenticate user identities, mostly for the purpose of payment or other financial transactions.[4] The process involves using the blockchain as another factor of security to create and verify the identity of users and facilitating management from the users' side, providing them more control over their personal information, who has access and how it is accessed. The US Department of Homeland Security recently awarded a grants to four projects that will utilize distributed ledger technology to develop new solutions for identity management and privacy protection.[5]

[4] "12 Companies Leveraging Blockchain for Identification and Authentication", Lets Talk Payments, 28 March 2016, https://letstalkpayments.com/12-companies-leveraging-blockchain-for-identification-and-authentication/.

[5] Giulio Prisco, "Department of Homeland Security Awards Blockchain Tech Development Grants for Identity Management and Privacy Protection", 18 August 2016, https://bitcoinmagazine.com/articles/department-of-homeland-security-awards-blockchain-tech-development-grants-for-identity-management-and-privacy-protection-1471551442

ABOUT GAMCROWD

GamCrowd was founded in 2013 when Chris North and Ian Hogg, two experienced gambling industry entrepreneurs, launched the first crowdfunding and crowdsourcing platform for the gambling industry.
Adjusting its model to respond to the market, GamCrowd closed the crowdfunding and crowdsourcing element of the business in late 2015. It now focuses on promoting the gambling technology sector to the wider tech community and covering tech trends that could be applied or disrupt the gambling industry. They do this through GamCrowd consult, GamCrowd news as well as the GamCrowd reports and events channels.

GamCrowd has become the home of the gambling technology sector holding monthly meet ups that cover topics like blockchain and Ai. With a community of over 4000 and growing GamCrowd aims to be the driving force of gambling technology development.

GamCrowd is also actively involved in start-up and early stage business focused events, GamCrowd Pitch ICE and the Launch Pad events at GIGSE and EIG with its partner Clarion Events.

In addition GamCrowd's tech week event as part of London Tech week looks at promoting the gambling technology sector to the wider tech community and to promote new tech trends to the gambling industry.

ABOUT CHAIN FINANCE

The mission of Chain-Finance is to examine and evangelise how different blockchains and distributed ledger technologies can enable and disrupt the global financial services industry. The team at Chain-Finance accomplishes this by providing research, intelligence, and education regarding the development of blockchain technologies for financial services and other industries. This includes producing events that bring stakeholders together, inform and educate about these new technologies, and encourage constructive discussions on how they can enhance services. The Chain-Finance team includes the following:

Dr. Hans Lombardo
Hans is a successful entrepreneur and enthusiastic analyst of new, disruptive technologies including blockchain technology, crypto-currencies, data analytics and Internet of Things. In 2012, Hans sold his previous company, a boutique research firm focused on Chinese high-technology industries. Hans is an Internet industry veteran with Asian regional c-suite experience. In the late 1990's, he earned tech journalist credentials at internet.com and Internet World magazine, interviewing Jack Ma, Jerry Yang, Vinton Cerf and Richard Li.

Adam Vaziri
Adam Vaziri is a director of Diacle, a firm that provides regulatory consultancy and compliance software for the fintech industry. Adam is also a founder of Bitlegal, an online directory and provider of information on regulatory landscape of bitcoin and blockchain technology. Adam is also a qualified solicitor and on the board of the UK Digital Currency Association.

Matthew Warner
Based near Windsor, England, Matthew is an enthusiast for innovative, cutting edge technologies. Matthew writes for Chain-Finance.com and AllCoinsNews.com. He is also a B.Eng. graduate in engineering with honours from the University of Warwick and a member of Mensa.

IF YOU WOULD LIKE US TO COME INTO YOUR COMPANY AND PRESENT THIS REPORT TO YOUR TEAMS THEN PLEASE CONTACT:

chrisnorth@gamcrowd.com

WE HAVE ALREADY DONE THIS FOR A FEW GAMBLING OPERATORS SO HAVE VARIOUS PACKAGES WE CAN DELIVER.

www.gamcrowd.com

click icon to visit our social media channels