GLOBAL COPYRIGHT REGISTER: **TECHNICAL PAPER**

COPYTRACK
GLOBAL COPYRIGHT REGISTER

ABSTRACT

The digital image and licensing industry is growing rapidly due to the proliferation of high-quality digital cameras. As a consequence, an influx of high-quality photography now exists in various untapped markets.

The market for digital images has a a few bottlenecks which have yet to be addressed. The commercial landscape makes the acquisition of photography costly for buyers. In addition, the process lacks transparency and is unprofitable for artists. The industry is controlled by only a few players who keep up to 70% of the revenue and leave rights-holders with little compensation.

Blockchain is a disruptive technology which has the potential to solve multiple problems in the rights-management industry: identification, u sage t racking, a nd o wner-management of digital content; smart contract payments to rights-holders; as well as transfer or sale of rights in part or whole.

The native token (CPY) will fuel the smart contracts that interact with the decentra-lized registrar. Due to the large number of hashes that can exist to identify digital con-tent, a new chain will be launched.

/// 1. INTRODUCTION

Since 2015, COPYTRACK has provided rights-holders with an overview of the usa-ge of their online creative works and com-bated illicit usage of their intellectual pro-perty. COPYTRACK has now emerged as the market leader and offers an effortless way for rights-holders to monetize their work.

Digital content management faces two types of challenges – those faced by users, and those faced by rights-holders. Users often misunderstand the usage of digital images online and the corresponding licen-sing options. In addition, they also lack ac-cess to licensing platforms and the ability to acquire usage rights in a timely manner.

On the other hand, rights-holders have few or no methods to prove ownership of original content and derivative work. Also, they often have inadequate tools to track the usage of their copyrighted images and identify violations. If a violation can be iden-tified, there are even fewer solutions avai-lable due to the global footprint of market participants.

Both users and rights-holders are faced with the challenge of reducing the cost of payments, so as to allow affordable purcha-se of use-rights for users and the maximiz-ation of revenue for rights-holders. In addi-tion, both groups struggle with facilitating seamless and timely settlement of pay-ments. These industry problems are further detailed in Section 2.

CopyTrack's solution is the creation of a distributed database and ledger whose core purpose is to store a decentralized copyright registry for digital content which authenticates users and links digital intel-lectual property. This registry will generate a unique ecosystem for rights-holders and open new, efficient markets. This paper de-scribes the functionality of the blockchain, including smart contract use cases, in Secti-on 3.

/// 2. KEY CHALLENGES OF DIGITAL CONTENT COPYRIGHT

While most professional photography is locked away in stock photography services and secured with watermarks, there is an increasing number of photos which are readily accessible on websites, social media and blogs without any information on avai-lable licenses.

This leads to a free-for-all mentality online with an estimated 85% of online images used without a valid license. Photos and images are copied and distributed without knowledge or consent of the rights-holders. This poses a serious problem to the indus-try; artists and creators suffer substantial financial loss due to undetected copyright violations.

2.1. User And Rights-Holder Challenges

Users are often unaware that any photogra-phy posted online without explicit licensing information, such as Creative Commons, comes with all rights reserved by the crea-tor. Even if the user is aware, there are high search and transaction costs: rights-holders are difficult to identify and contact, and it is a time-consuming endeavor to negotiate and acquire appropriate licensing rights.

Rights-holders are usually unaware of the copies of their content used worldwide, and therefore are unable to act on violations.

Artists are not keen on tracking their work and validating licenses. Rather, they are looking for a service that can facilitate this for them. Stock photography sites provide some of these services; however, they leave artists with an unfair share and keep up to 70% of revenue for themselves.

2.2. Global Nature of Digital Assets

The challenges outlined previously are glo-bal in nature and are common to all areas of digital content. The marketplace is highly fragmented: almost all current methods for infringement resolution are based on nati-onal legal frameworks and tools. These fra-meworks typically present insurmountable barriers for individuals to overcome unless they enlist professional help.

Lastly, these facts and figures only refer to the digital image market and the illegal use of images online, yet there are nume-rous categories of digital content where the same patterns apply: video content, music, and text, as well as notary and legal docu-ments.

/// 3.
WHY BLOCKCHAIN?

The concept of using the Bitcoin block-chain to notarize data by publishing a hash of the data in a Bitcoin transaction is not new [1]. As such, it is easy to see that the core model of the decentralized registrar is to create a database to store the current and historical information about digital content: its identifying hash, the public key of the owner and past owners, and the pay-ment history to the rights-holder by anyo-ne who uses the registered digital content. Smart contracts are used to modify the sta-te of the digital content.

A smart contract can interact with or modify digital content in three ways. First, users can seamlessly pay rights-holders to use their digital content. Also, rightsholders can transfer ownership or codify different rights. The native token is used as a payment to execute the various smart contracts. The methodologies for each of these interactions are described more fully in Section 3.3.

At its current performance, Bitcoin can handle about five transactions per second, and each transaction costs approximately $0.50 USD [2]. Because of this limitation, it becomes economically infeasible to integrate large volumes of data for pre-existing digital content on the Bitcoin, or any platform's, blockchain.

Due to the current total number and future projections of available digital media (see Figure 1), it is necessary to develop a highly scalable method to store a large amount of identifying hashes in a custom blockchain built for this specific task.

Details of the Proof-of-Stake consensus protocol can be found in Section 3.1. To achieve high scalability, the ledger balance will be stored as Unspent Transaction Outputs (UTXOs), which are discussed in Section 3.2.

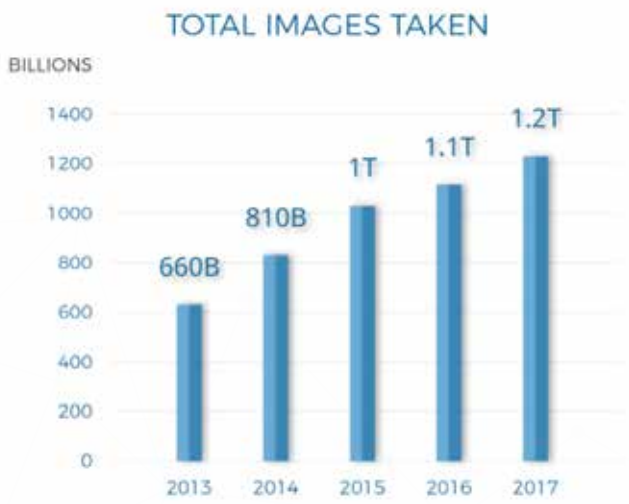

Figure 1. The digital image market is growing rapidly worldwide. InfoTrends latest global forecast of photos taken estimates that the total number or images stored in 2017 is around 4.7 trillion. The data reveals a staggering 1.1 trillion photos were captured by mobile devices and still cameras in 2016. This number will grow to over 1.2 trillion in 2017, and 1.4 trillion in 2020 with a Compound Annual Growth Rate (CAGR) of 9%.

3.1. Consensus protocol

We choose Proof-of-Stake (PoS) as our consensus model for many reasons which relate to problems inherent in Proof-of-Work (PoW). First, obtaining proper decentralization while achieving an unbounded solution to the Byzantine Generals' problem via Proof-of-Work, also known as Nakamoto Consensus, requires the calculation of a non-trivial computationally intensive problem. Often such problems are memory-bound or bandwidth-limited. In other words, the time to solution is related to the speed and size of the memory bus. The larger and faster the memory bus width is, the more efficiently the algorithm can perform. As a natural consequence, bitcoin mining, which currently uses the SHA-256d hash as PoW, evolved from first running on CPUs to GPUs as specialists ported the algorithm of the hash function to run on GPUs. Eventually, Field Programmable Gate Arrays (FPGAs) were used to prototype the first custom Application Specific Integrated Circuits, or (ASICs), with each generation being more efficient than the last. Numerous algorithms have followed the same development process as SHA-256d.

Due to economies of scale, large mining operations are more efficient than smaller ones. One could argue that the development of ASICs exacerbated this threat to decentralization. Still, large GPU farms convey the same threats as ASIC farms, i.e. those due to mining centralization. One cause of centralization is the availability of the GPUs on the retail market. Currently, a worldwide shortage of GPUs exists,
as can be seen by lack of availability. This is most likely due to the unforeseen demand for GPUs in cryptocurrency miners caused by the rapid increase in the market capitalization of GPU-minable coins.

On the other hand, various Proof-of-Stake models provide a similar level of security in the same manner as Proof-of-Work. However, the original PoS model suffers from coin-age attacks and is now rarely used. Ignoring any academic PoS models, such as Snow White [6] or Sleepy [6], as few open-source projects have put these into practice, the state of the art is PoS 3.0, as detailed by the Blackcoin developers in [3]. PoS 3.0 theoretically rewards node operators which stake their coins longer while giving no incentive to coin owners who do not participate in securing the network and leave their wallets offline. As such, the PoS 3.0 consensus model has been chosen for our blockchain.

3.2. UTXO

The UTXO model consists of a forest structure that tracks the history of a unit. Roots are coin-creation events, such as rewards obtained from PoW or PoS, and have no input transactions. By definition, all leaves are unspent transaction outputs. When a leaf branches or sprouts a new limb, the leaf becomes an inner node of the graph. During this process, the unspent transaction output is consumed and used as the input of a new unspent transaction output. Using this model, one can transparently trace back the history of each transaction through the public ledger. The UTXO model inherently allows for parallel processing capabilities to initialize transactions among multiple addresses, indicating its scalability.

The current industry leader for smart contract platforms is Ethereum, which uses Solidity – a Javascript-resembling Turing-complete language, for coding smart contracts. Despite a flaw in the Parity Wallet written in Solidity and the DAO attack, Solidity is currently the leading smart-contract language. For this reason, smart contracts for our blockchain will be Ethereum Virtual Machine (EVM) compatible.

Different from the UTXO model, Ethereum is an account based system [5]. In that design, each account experiences direct value and information transfers with state transitions, similar to a real world bank account. Every newly generated block GLOBAL COPYRIGHT REGISTER: TECHNICAL PAPER 5 potentially influences the global status of other accounts. Every account has its own balance, storage and code-space base for calling other accounts or addresses, and stores respective execution results. In the existing Ethereum account system, users perform P2P transactions via client remote procedure calls.

Although sending messages to more accounts via smart contracts is possible, these internal transactions are only visible in the balance of each account; thus, tracking them on the public ledger of Ethereum is a challenge. Because of these limitations, Ethereum currently suffers from a scalability bottleneck and isn't suitable for the core usage of our proposed global registry. Co sequently, we will adopt the innovative design of Bitcoin-network UTXO model.

3.3. Content as a Smart Contract

We introduce the notion of „Content as Smart Contracts." When content is recorded on our blockchain, it will be included in the database as a smart contract, with a state that initially contains several pieces of information: 1) a hash of the digital content, and 2) the (hash of the) public key of the content owner.

The history of the state of the registered content is then stored automatically in the blockchain database. The state of the content is updated with the hash of the appropriate message signed with the private key which corresponds to the public key of the current owner. For instance, changing the ownership of the content can be done by hashing a signed message which contains the new owner's public key and the amount of CPY for the sale. Owners of registered content can also be paid seamlessly by deriving a fixed address from their public key for all payments.

In order to execute a smart contract, a dynamic amount of CPY must be used as payment, akin to Ethereum's and Qtum's gas model. Payment is not necessary for registering content as content creators and rights-owners will go through our KYC process to prove they have they right to register content.

By utilizing trustless smart contracts and defining atomic functions that can change the state of the content, we can eliminate costly middle men. Content registration, proof of ownership, and payment to copyright holders has never been easier.

REFERENCES

[1] M. Araoz. What is Proof of existence?, (2014). http://www.proofofexistence.com/about

[2] Transaction Fees - Bitcoin Wiki, (2017). https://en.bitcoin.it/wiki/Transaction_fees

[3] BlackCoin: The Original Proof of Stake Coin. http://blackcoin.co/

[4] Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform. https://qtum.org/en/white-papers

[5] A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper

[6] P. Daian. Snow White Robustly Recon gurable Consensus and Applications to Provably Secure Proofs of Stake, (2016). https://eprint.iacr.org/2016/919.pdf

[7] R. Pass. The Sleepy Model of Consensus, (2016). https://eprint.iacr.org/2016/918.pdf