Smart Contracts - Smart and Stupid Applications on the Blockchain

Fabiola Buschendorf
Department of Computer Science
University of Goettingen, Germany
f.buschendorf@stud.uni-goettingen.de

***Abstract*—The blockchain technology offers the implementation of decentralized systems such as cryptocurrencies or smart contract execution. Bitcoin and Ethereum are popular blockchains, offering distributed services in peer-to-peer networks between untrusted members. Though this technology has many advantages, current applications seem to exceed their transaction capacities. Security breaches and re-centralization are contradicting a blockchains original purpose. New ideas on the blockchain generate high amounts of funding, without ensuring actual profits for investors. This paper analyses the capabilities and limits of current blockchain technologies. It will then evaluate future applications and discuss possible benefits from decentralization. We work out essential criteria future blockchain applications should fulfill in order to contribute in a meaningful way to current systems.**

***Index Terms*—Blockchain, Cryptocurrency, Bitcoin, Ethereum, Smart Contracts**

I. Introduction

BLOCKCHAIN applications are popular since the cryptocurrency *Bitcoin*, developed by Satoshi Nakamoto, went public in 2009 [1]. The coins are exchangeable in a decentralized network, thus independent from central authorities. The blockchain technique provides a nearly immutable data structure for coin transactions. By appending new blocks to the current chain and propagating this information over the network, every node has an overview of current balances.

Alternative currencies, named *altcoins*, started spreading with different application purposes either building on top of the Bitcoin protocol or developing an own system of the distributed transfer book. The first altcoin, *Namecoin*, aims to provide an independent naming system for top-level domains [2], motivated by the shut down of secret-leaking sites by the U.S. government [3]. The idea of using the blockchain technology for various purposes was accelerated by *Ethereum* in 2013, initiated by Vitalik Buterin and developed by the Ethereum Team [4]. It established a network capable of executing small programs, called *smart contracts*. Converting the digital currency *Ether* to *Gas* these programs can be executed and verified by each participant, diminishing the need of a trusted third party. Though decentralization can contribute to the transparency and security of transactions and contracts, a blockchain is not a universal remedy. Current block sizes are limited and block creation can be time and energy consuming. Further, the Bitcoin blockchain reached a size of 140 GB by November 14th 2017 [5], impeding the participation in the network.

By the time of this writing, Bitcoin has a market capitalization of 122 billion US$ [6], creating a spot of attention around its technology and thereby motivating researchers, developers and companies to create profitable applications on top. Firstly, Section II provides an introduction to the technology behind any blockchain application. Advantages as well as restrictions of the blockchain technique are discussed in Section III. Section IV gives examples of current applications and analyzes their shortcomings. We examine how future implementations plan to solve the problems inherent to huge blockchain networks in Section V. We discuss which of the new technologies might be revolutionary and which proposals simply try to jump on the train of success.

II. Blockchain Technology

A blockchain is a data structure referencing its ancestor, similar to a back-linked list, see Figure 1. Each block contains information about several transactions and a header. In Bitcoin an average block carries 500 transactions, resulting in a block size of 1 MB [7]. The chain is kept redundantly on each participants computer in a *peer-to-peer* (P2P) network. The task of these nodes is to verify the correctness of each transaction and to bundle pending transactions into new blocks. A *consensus* is reached if every node accepts a newly created block and updates its chain.

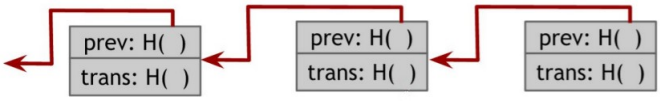

Fig. 1: A blockchain containing transactions and referencing its parent [8]

Each block is identified by a hash on its header. The block header contains a field for the previous blocks' hash, the protocol version, a timestamp, a reference to the block's transactions and information about the mining process. *Mining* refers to the act of adding a block to the chain and verifying transactions. This process is commonly designed as a difficult puzzle, limiting the ability of any one party to control the consensus process. This puzzle is time and energy consuming, so the *incentive* for a participant to mine a block is a reward in form of the networks currency (Bitcoin, Ether, ...) or token. This mining principle is called *proof-of-work*, but in Section V

an alternative is described. Once a block is mined and verified, the nodes start building on top of it. In the case two nodes solved the puzzle simultaneously, the consensus is to accept the longest new chain, so each node has to build another block on top of the newly created one in order to convince the network to accept its mined blocks and to receive the reward [7].

As the verification of hundreds of single transactions can be tedious, another useful data structure is used: A binary tree called *Merkle tree*. In a Merkle tree each data point, e.g. a transaction, is hashed and grouped into pairs. The hash of each of these pairs is taken and stored in a parent node. The parent nodes are grouped in pairs again, hashed and stored one level up the tree [8], see Figure 2. A single hash results and is stored in the block header as the Merkle tree *root*. The verification of the existence of a single transaction is now possible in $log(n)$ steps, if n transactions are included.

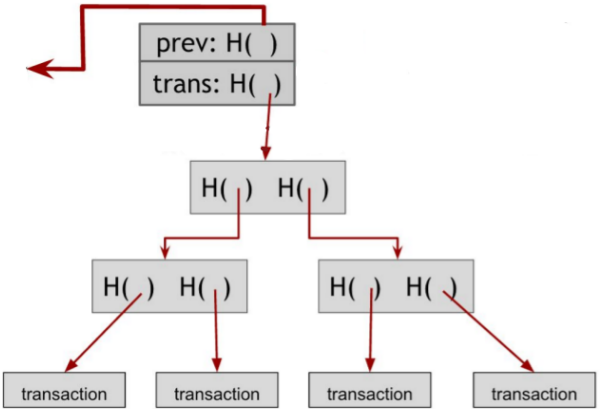

Fig. 2: A Merkle-tree referencing the blocks transactions [8]

This data structure is living in a public or private P2P network. Each participant, referred to as *node* holds a copy of the blockchain and has equal power. Bitcoin, for example, is a public network in which everyone can take part by downloading a client software and start trading or mining. The common data storage model relies on centralized servers which distribute data to several clients. In the next section we evaluate these principles.

III. Blockchain Features

In this sections advantages as well as constraints of a blockchain are discussed. These features are important to further analyze which applications might or might not benefit from a blockchain.

A. What can be done

As we already state in Section II, a blockchain is living in a decentralized P2P network. The clients do not rely on a central server. This removes the occasional downtimes of single servers, or delays due to heavy traffic. Further, there is no *single point of failure* which might be attractive to data thefts.

Sharing data does also contribute to the *transparency* of a system. It facilitates trading with untrusted partners, as each entity can verify the transactions itself. While in common banking system a bank offers the service of a trusted third party between two trading partners, the need of a mediator vanishes in a blockchain system. This reduces first transaction fees and second the need of a trusted central authority.

Another feature of a blockchain is the *immutability*. When blocks are mined and adopted by a majority of the network, they cannot be changed or substituted. The consensus mechanism is the basis of a order of transactions everybody agrees on, see Section II.

In terms of *privacy* protection a blockchain might be advantageous, because instead of keeping the data on a single server, it can be widely distributed and verifiable encrypted.

B. What a Blockchain cannot provide

As well as a blockchain might improve the privacy, also weaknesses of the data structure are to be mentioned. How can a distributed and transparent system be more privacy preserving than a central database? Even tough the latest cryptographic practices are being used in modern blockchain applications, history teaches us that such algorithms might get broken by sophisticated hardware or due to design faults. In addition, human errors such as inappropriate key handling or careless implementation cause data security risks. Though it is important to mention the existence of Zero-knowledge proofs, which is a cryptographic construction where one can prove possession of a piece of data, e.g. a secret key, without revealing that information to another party [9].

But most importantly, the main concern in blockchain technology is its lack of *scalability*. This refers to both: Processing speed and data size. In order to run a full node, users of the Bitcoin Core client would have spend in 2013 an average of 2 days to download the (at that time) 16 GB chain and verify it [7]. Moreover, an average block contains about 500 transactions and a new block is mined every 10 minutes in Bitcoin and every 14 seconds in Ethereum on average, with the highest number of 546.837 transactions on Friday, October 20, 2017 [10]. In comparison, the VisaNet processes 150 million transactions on a daily average in 2010 [11]. Therefore, applications that require fast transactions with large amounts of data might not be suited to the current capabilities of blockchain designs. Figure 3 shows the number of pending transactions in the Bitcoin memory pool, which has its peak sizes either when lots of transactions are requested at the same time or in case the hash difficulty has been raised and mining pools dropped out of the network at the same time. Bitcoin price boosts may have been an issue causing the hight peak in May 2017. Figure 4 depicts the evolution of Bitcoins chain size. These charts underline the scalability problem of a matured blockchain.

It is further important to notice that tough *immutability* provides safety to the system, it also hardens to updates a blockchain application. As every node needs to run the same software for consensus, mining, chain state and verification, an incompatible change (a *hard fork*) to the architecture would

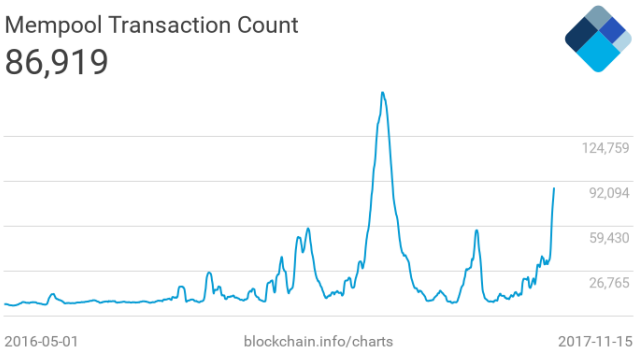

Fig. 3: Number of pending transactions in the Bitcoin blockchain [12]

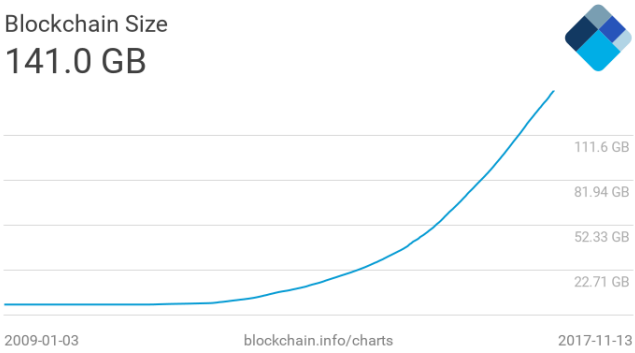

Fig. 4: Growth of the Bitcoin blockchain [12]

require every node in the network to accept, download and deploy the update.

All these issues impede the *longevity* of a blockchain network. It is questionable if a long-lasting and always-secure system can be achieved by an application which does not offer easy update mechanisms and does not scale well.

IV. Existing Applications

In this section past and current blockchain applications are examined and their difficulties are evaluated referring to the features a blockchain can offer.

A. Services of current applications

As the previous sections are discussed using Bitcoin as a running case, this section focuses on examples of more recent or alternative technologies: Namecoin, Ethereum and extending smart (or stupid) applications such as *Storj*, Decentralized Autonomous Organizations (DAO), Initial Coin Offerings (ICOs) and *Useless Tokens*. Many of these applications are based non-academic ideas, for the reason that up-to-date research work is not available at this time. The mentioned services are selected as they either belong to the most popular ones or are based on interesting ideas.

1) Ethereum: Ethereum developers describes Ethereum like this: "Ethereum does this by building what is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications [...]."[4].

Smart contracts can be build on top of the platform. They execute code written in a turing-complete scripting language and can send messages to other contracts or accounts owned by external users. Every message is part of a transaction, which identifies its sender and recipient, an amount of the cryptocurrency *Ether* which should be passed and a STARTGAS value, representing the maximum number of computational steps the code execution is allowed to take. *Gas* is Ethereums internal value, paid in order to prevent accidental or hostile infinite loops or other computational wastage in code. There is also a fee of 5 gas for every byte in the transaction data, reducing the consumed storage resources. The code of each contract is stored in the Ethereum blockchain and is executed by all nodes as part of the block validation process. Thereby, once a transaction is launched, it is acting autonomous.

These code-written contracts can be used to facilitate, verify, and enforce the negotiation between untrusted agents [13]. The publicity of the code can potentially circumvent censorship, collusion, and counter-party risk, ensuring that the business partner will live up to its contractual obligations.

Buterin proposed several possible applications running on top of the Ethereum blockchain. Many of those have been realized already, such as The DAO and Storj, which we examine later. Ethereum defines a standard for tokens traded on its blockchain, specified in the ERC20 token standard [14]. It is possible to create an arbitrary number of token, with a specified value and to sell them as a fungible good to customers interested in market shares or voting rights within the token offering organization.

The main differences to Bitcoin are: Faster block creation time, future implementation of an alternative consensus algorithm (*proof-of-stake*, see Section V) and a turing-complete language.

2) Namecoin: Namecoin is the first altcoin, launched in 2011 [8]. Namecoin aims to provide a decentralized Domain Name System (DNS) by putting name/value pairs in a blockchain [2]. The name is the domain a user wants to register and the value field contains configuration options, such as the IPv4 and IPv6 addresses. The websites are accessed using the pseudo TLD `.bit`. The name `d/mysite` represents a record stored in the DNS namespace `d` with the name `mysite` and corresponds to the website `mysite.bit`. A browser extension or a special client software acts as a local DNS server and look up the address from the shared blockchain instead of the traditional DNS [15]. Using the cryptocurrency Namecoin (NMC) one can register, update and transfer domains. The current registration fee is 0.01 NMC and some amount of transaction fee is given to the miners as a reward, jut like in Bitcoin. A higher fee improves the chance that the transaction will be processed quickly.

The Namecoin blockchain is a hard fork of the Bitcoin

software and uses the same proof-of-work algorithm. But Namecoin adds a few new rules to its system. For example, it is possible to update domains by submitting a new transaction with the same name and modified values. Only the owner of the domain, e.g. the associated private key, is allowed to create such updates.

The motivation of Namecoin was that a central authority managing domain names, such as ICANN, requires too much trust in a single entity and represents a single point of failure. Some incidents which accelerated the research for decentralized alternatives are listed in a survey on Namecoin by H. Kalodner et. al. [16]: Firstly `wikileaks.org`, leaking the *Iraq War Logs* had been shutdown by U.S. DNS providers in 2010 [3] and secondly the U.S. Department of Justice had seized 82 website domains which traded counterfeit goods in the same year [17].

3) Cloud storage: Cloud storage is massively used in centralized services as for example Dropbox, Google Drive or ownCloud. Several services offer distributed storage, where meta information about the data is stored on a blockchain. As an example, the service *Storj* is examined.

Storj is a cloud storage provider, using the P2P network structure to transfer and share data without reliance on a third party storage provider. It implements client-side encryption, scatters chunks of data redundantly among its users and therefore claims to reduce data failure and outages. A challenge-response verification system ensures that only the owner of the data can access it. Like other decentralized applications, data on a network will be resistant to censorship.

Currently Storj implements its platform on the Ethereum blockchain. Data storage is negotiated via a contract, which describes the relationship between data owner and storage owner. Payments and data transfers is regulated by this contract, while the user pays with STORJ tokens for storage space. Data chunks are stored as shards in multiple locations and Merkle trees are used to proof the retrievability of a piece of data on a machine [18].

The idea of decentralized data storage has been popular since the early 2000's, when the BitTorrent protocol became popular. BitTorrent focuses on file sharing in a P2P network [19], while file contents in Storj are hidden from the public network. Another similar project is *Filecoin*, ending its token sale in September 2017 and having raised more than 205 million US$ [20]. Additionally, the Open Source protocol InterPlanetary File System (IPFS) aims to create a distributed file system to share and store web content [21].

4) DAO: Decentralized Autonomous Organizations were proposed by Ethereum developers in the Ethereum Whitepaper [4]: "[...] a DAO is a virtual entity that has a certain set of members or shareholders which have the right to spend the entity's funds and modify its code. The members would collectively decide on how the organization should allocate its funds.". The blockchain would operate as a digital ledger and track the organizations financial interactions. The absence of a central authority in blockchains would make the DAO independent from states and reduce the risk of charity fraud. It also facilitates the decision making process by allowing *liquid democracy*, where the organizations members vote for delegates who then execute a vote. Anyone can act as a delegate, the term lengths are flexible and the delegate's power is decided in the voluntary choice of the organizations members rather then a predefined juristic system [22]. These mechanisms are implemented and executed by smart contracts.

An example is *The DAO*, which was a form of investor-directed venture capital fund, founded in 2016 [23]. The DAO's code was open source and got quickly adapted into the Ethereum blockchain, attracting nearly 14% of all ether tokens issued to May 2016 [24]. Investors could participate and vote on the directions of the organizations investments. Volunteers curated project offers and the submitters identity to ensure the proposed projects were legal. On June 2016 The DAO was attacked, exploiting a flaw in The DAOs code which was previously discovered by researchers. Because of the big share The DAOs tokens had of the Ethereum blockchain the community decided to recover the stolen tokens, thus creating a hard fork of the Ethereum blockchain which resulted in a split of the cryptocurrency [25]. This created a huge controversy, which is discussed in Section IV-B.

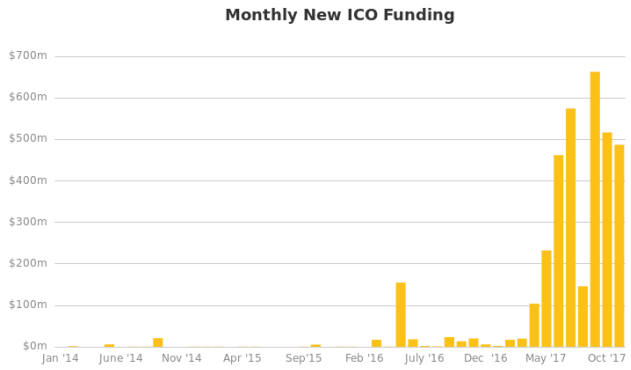

Fig. 5: Monthly new ICO funding [26]

5) ICO: Initial Coin Offerings are a mean to crowdsource projects and to distribute rights or access to a future technology. Such projects offer tokens representing a smart property, coupons or point systems for their products. This procedure is similar to initial public offerings (IPO) where investors gain shares in the ownership of an established company on the common stock market. In contrast to IPOs, ICOs are not governed by laws and do not require legal actions such as the contraction of investment banks or the disclosure of financial and business information [27]. This reduces legal and accountability costs and thereby making the ICO a popular approach for startups. A common practice is to publish a Whitepaper, describing technical details as well as the business model to convince possible investors, though the stated procedures in a Whitepaper are not legally binding. The development of Ethereum was financed by an ICO and raised 20 million $US in 2014 [8] and Filecoins ICO in September 2017 raised a sum of more than 205 million US$ [20]. Figure

5 shows that funding in ICOs became more and more popular.

6) Purposeless Currencies: The most market capitalizing currency without any particular vision is Dogecoin. It is a parody of cryptocurrencies, created in 2013 [28]. It is operating on an own blockchain derivated from Bitcoin, mining a new block every minute without a finite number of coins. It uses a different proof-of-work algorithm than Bitcoin, making it complicated to use dedicated hardware devices for mining. The current per-block reward is 10.000 Dogecoins, which produces around 5.2 billion new coins per year, thus inflating the coins. The name *Doge* is referring to the internet meme of a Shiba Inu, whose popularity could attract the interest of a large community. The Dogecoin community is encouraging fundraising for different projects, such as the Jamaican Bobsled Team, which had qualified for the 2014 Winter Olympics [29], but could not afford to go to and the sponsoring of a NASCAR driver. Additionally, different tipping services had been crated, used to support individuals on Reddit or Twitch.tv [30]. While Dogecoin has its justification, the *Useless Ethereum Token* doesn't. In June 2017 it collected 113.247 $US during its ICO, though being honest with its uselessness: "The UET ICO transparently offers investors no value, so there will be no expectation of gains." [31].

B. Their Complications

The approaches elaborated in the previous section have been developed and deployed in the last decade. Some of these novelties had reached serious performance limits, suffered security breaches or caused questionable practices on the edge of legality and social justification.

1) Scalability: We examine in Section IV-B, that processing speed and storage capability of a blockchain are limited. Regarding the speed of transactions, digital currencies cannot process the volume required by a large economic society. Payments often need to be verified in seconds (Supermarkets, Restaurants, Shops, ...). If blockchains are growing too large, a majority of nodes stops verifying actual blocks but adapting to a more lightweight chain, therefore promoting the formation of commercial, centralized "big" nodes. Moreover, the more transactions are pending in the Mempool chain, the more expensive are transaction fees in order to incentive miners to accept the payment quickly [8]. In Section V we examine a solution offered by the *Lightning Network*.

2) Immutability: Once the code for a smart contract is uploaded to the blockchain and adapted by the majority of nodes, it cannot be reversed. This is an important security mechanism, but has the downside that flaws in smart contracts cannot be corrected. The hack of *The DAO* showed that security lacks can cause serious damage. In June 2016, two months after its code has been launched, The DAO was subject to an attack that exploited a combination of vulnerabilities, which were discovered by researchers before. A third of The DAOs tokens, around 3.6 million Ether had been stolen. This lead to a hard fork of the Ethereum blockchain, as the consequence of a split of the community, where a minority of Ethereum miners remained on the un-forked chain, called *Ethereum Classic* [25]. This underlines the importance of update mechanisms to facilitate the maintenance, management and longevity of a blockchain. In Section V we examine an idea which allows to correct errors in smart contracts.

3) Proof-of-work and Consensus: The core of the difficult computation Bitcoin miners are working on is the SHA256 hash function. This function needs to be recalculated as fast as possible until it falls below a certain *difficulty*. This requires specific hardware, as CPUs of general purpose computers are not efficient anymore. Thus, application-specific integrated circuits (ASICS) have been specially designed and produced for time intensive mining. Professional mining centers arose, buying slightly newer and more efficient ASICS at bulk price. The ASICS need to be cooled and require a huge amount of electricity. Estimations reported in 2015 the whole Bitcoin network was consuming around 10% of a large power plants worth of electricity [8]. To circumvent this specialization, ASIC-resistant puzzles have been designed. Ethereum implements a memory-hard puzzle, which requires a large amount of memory, making GPUs best suited for mining. Current GPUs are already highly optimized, thus potential specialization gains are low [32]. But this is not the only problem in nowadays mining puzzles.

As the costs for mining had increased to a level where individuals could not afford mining anymore, the formation of *mining pools* was motivated. Miners collectively mine for blocks and share their rewards based on the work each participant actually performed. In Figure 6 one can see the share of the biggest Ethereum mining pools for the mined blocks during 24 hours in November 2017. Some mining pools concentrate more than 20% of the total network mining power, which somehow violates the idea of a decentralized currency. Moreover, if any pool gains 51% of total mining power, it could basically control the network by agreeing on an own consensus [8].

A better mining puzzle should reduce energy costs, be ASIC-resistant and discourage the formation of mining pools. In Section V we examine a solution offered by *proof-of-stake* algorithms.

4) Complexity: A complex language or deployment mechanisms can draw possible users back from a blockchain application. In Namecoin, an empirical study by H. Kalodner et. al. showed that from nearly 200.000 registered domains, only 9354 resolved to an IP address and merely 28 pages were serving non-trivial content that was uniquely available via .bit. It prove, that 76% of domains were reserved by *squatters*, reserving names in order to sell it one day with a high profit, or pages consisting of only a few words like "Welcome to mysite.bit." [16]. The researchers conclude that a poor usability of Namecoins client software, long setup times and tedious maintenance of .bit domains cause the low usage of Namecoins intended service.

Another usability hurdle has to be taken writing smart

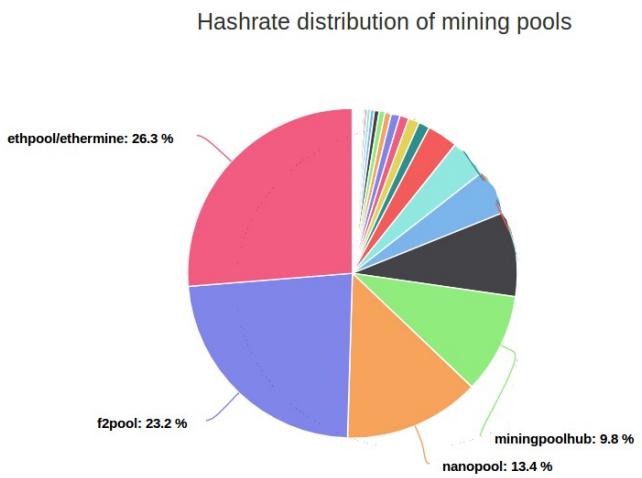

Fig. 6: Share of mined blocks in Ethereum by mining pool last 24 hours, December 2nd 2017 [12]

contracts, which is done in one of Ethereums high-level programming languages Serpent or Serenity. Both require profound coding knowledge, making it impossible for most marketers or lawyers to setup flawless contracts. And as we know, errors in the blockchain cannot be corrected. In Section V we examine ideas which claim to offer a better usability on smart contracts.

5) Scam: The popularity of ICO funding and the lack of ICO regulation attracted fraudsters, publishing promising Whitepapers and disappearing with huge amounts of Ether generated in token sales. Additionally the value of a cryptocurrency or token is based on their popularity, thus token values are underlying a huge fluctuation. Currently, ICOs are a highly risky way of investment, as no solid company goods but ideas are being funded. A solution can only be found by politics.

V. Future applications

Researchers and developers of smart applications are aware of the bottlenecks explained in Section IV-B. Future applications aim to correct current flaws, or propose new areas of operation for the blockchain technology. In this section we discuss those proposals while considering the benefits and drawbacks examined above.

The *Lightning Network* enables a network of Bitcoin micropayment channels whose transfer of value occurs off-chain. It claims to reduce transaction fees for small payments, process a large amount of transactions in real time using Bitcoins build-in scripting language. Smart contracts are established between multiple parties, creating a network of nodes which forwards packets of transactions similar to packet forwarding in IP networks. Its fundamental technology is a local two-party consensus. Two parties allocate a balance into a multisignature transaction, which can be updated only if both partners cooperate. They may continue updating states without interacting with the global blockchain until they wish to close the channel and only the most recent state is broadcast. Many of such channels can be opened simultaneously and intermediate nodes do not need to be trusted [33]. The main criticism about the Lightning Network is that in order to work well it requires centralized hubs, which contradicts Bitcoins idea of an independent and decentralized network [34].

A solution to mining centralization and hardware specialized mining is possible by *proof-of-stake* (PoS) algorithms. In PoS, a set of nodes (validators) take turns voting on the next block, and the weight of each validator's vote depends on the size of its deposit (i.e. stake) . A PoS algorithm does not require a huge amount of computation, thus the mining process will be more energy conserving. Ethereum aims to implement a PoS algorithm called Casper in the near future [35].

Though thoughtful fixes and new techniques can improve established blockchains such as Bitcoin and Ethereum, developing a new technology might deliver better overall performance. Taking the idea of smart contracts a step further, *Agrello* proposes a system of self-aware smart contracts (SAC) [36]. It adds obligation constructs for execution and enforcement of contractual obligations and facilitates updates to existing contracts. Obligations and rights are essential in legally binding contracts and are specified in a human readable markup language. A user interface is provided to enable unexperienced users to setup contracts. Several stages in smart contracts have been put into templates, including a setup phase and eventual rollbacks if obligations are breached or faulty information is delivered. External events can be handled by the contract itself. Current problems caused by the immutability of smart contract frameworks require a management of the contract setup phase. This process is described as *lifecycle management* in [37]. During the negotiation dissent and counter-offer or consent are possible outcomes and possible exceptions are considered. The contract code itself, when broadcast to the blockchain, remains immutable but trough an easier usability, possible rollbacks and by including external events the contract gains flexibility and fault tolerance.

Regarding new areas of operation, three academic proposals are investigated. In [38] the author suggests a currency system for academic peer review payments using the blockchain technology. The problem of academic peer review is a lack of quality, poor reviews from competing institutions or insufficient willingness to contribute reviews. The currency system aims to provide a greater incentive to carry out qualitative peer review and tracks the review process. On-time reviews are rewarded with coins and in turn can be spend to submit own papers for peer review. This technique would also allow for automatic recognition of peer review activity, such as the journal and year of review by tracking the coins origin. Journal editors rate submitted reviews and reward authors by the reviews quality. In this proposal, journal editors

do possess a centralized role, e.g. they need to be trusted entities. How these editors are elected or how new journals are accepted to the review system is not clarified by the article. However, it is important to prevent the formation of fake-journals, in which untrustworthy editors generate coins for dishonest reviews. More importantly, this paper underlines that the main advantage of a blockchain is the decentralization of power, but the proposal in [38] includes trusted entities: the editors. A coin reward system might be better allocated in a transparent database which can operate faster and possibly store additional chunks of information attached to a review-coin, such as the reviewers history. However, also peer-review might benefit from decentralization, especially if this could improve access to and quality of independently published research work and open-knowledge.

In [39] the authors suggest self-managed and blockchain-based vehicular ad-hoc networks (VANETs). VANETs are a current subject of research for vehicle to vehicle communication, in order to warn about traffic jams or accidents and to obtain information from road side stations about weather conditions. Moreover, this infrastructure can detect speeding cars and enforce certain punishments. The article suggests to decentralize VANETs, thus reducing government surveillance and diminish risks of single points of failure. Management of tax and insurance payments could be executed via smart contracts on the Ethereum blockchain, which would reduce bureaucracy. The article further proposes to implement traffic regulation applications and to identify misbehaving cars. This proposed network would indeed benefit from decentralization and smart contract automation. However, if joining is not mandatory it is to be questioned if the benefits for car owners through participating in this network compensate the costs. Many of the implemented information services are already available for free, by radio or smartphone applications. Additionally it is important to mention that this proposal does not offer solutions to important VANET functions, such as car distance information and very recent accidents. These services require high information processing speed which cannot be offered by Ethereum yet.

A third paper discusses secure encryption of anonymous partners over the Bitcoin blockchain. While payment can be processed protecting the users pseudonimity, communication after transactions isn't independently secured in a decentralized manner. The researchers propose a Diffie-Hellmann-over-Bitcoin Protocol where a shared secret is generated using signatures from two previous transactions. The authors prove the secrecy of the partners private keys as well as their shared key. Integrity of the signatures is provided through the blockchains immutability. The key generation does not require interaction, however the secrecy of session keys used in the past is not guaranteed. [40]

VI. Conclusion

In this paper we have evaluated current blockchain applications and pointed out the lack of scalability and usability as well as the drawbacks of immutable smart contracts. We underlined negative side effects of blockchains current popularity such as scams and re-centralization. We analyzed how future applications aim to accelerate transactions, add security mechanisms, improve smart contract usability and lifecycle-management. Some academic proposals for new blockchain application areas were discussed and following essential criteria has been worked out for potentially successful applications: The underlying system should benefit from decentralization, solve a real problem, offer usability features, include correcting mechanisms for contracts and require a medium transaction speed.

References

[1] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. URL: https://bitcoin.org/bitcoin.pdf (2008). (Accessed November 3, 2017).

[2] Durham, V. Namecoin Github repository. URL: https://github.com/vinced/namecoin (2011). (Accessed November 3, 2017).

[3] Mutton, P. WikiLeaks.org taken down by U.S. DNS provider. URL: https://news.netcraft.com/archives/2010/12/03/wikileaks-org-taken-down-by-us-dns-provider.html (2010). (Accessed November 16, 2017).

[4] Wood, G. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. URL: http://gavwood.com/paper.pdf (2014). (Accessed November 29, 2017).

[5] Blockchain.info. Blockchain size. URL: https://blockchain.info/de/charts/blocks-size (2017). (Accessed November 3, 2017).

[6] Coinmarketcap. Cryptocurrency market capitalization. URL: https://coinmarketcap.com/ (2017). (Accessed November 3, 2017).

[7] Antonopoulos, A. M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (O'Reilly Media, Inc., 2014), 1st edn.

[8] Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton University Press, Princeton, NJ, USA, 2016).

[9] Company, Z. E. C. What are zk-SNARKs? URL: https://z.cash/technology/zksnarks.html (2017). (Accessed November 30, 2017).

[10] etherscan.io. Ethereum pending transactions queue. URL: etherscan.io/chart/pendingtx (2017). (Accessed November 14, 2017).

[11] usa.visa.com & IBM. Visa acceptance for retailers. URL: https://usa.visa.com/run-your-business/small-business-tools/retail.html (2017). (Accessed November 14, 2017).

[12] blockchain.info. Confirmed transactions per day - Chart. URL: blockchain.info/charts (2017). (Accessed November 14, 2017).

[13] Szabo, N. The Idea of Smart Contracts. URL: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html (1997). (Accessed November 15, 2017).

[14] Wiki, T. ERC20 Token Standard. URL: https://theethereum.wiki/w/index.php/ERC20_Token_Standard (2017). (Accessed November 16, 2017).

[15] Wiki, N. Namecoin DNS Specification. URL: https://wiki.namecoin.info/index.php?title=Domain_Name_Specification (2017). (Accessed November 16, 2017).

[16] Kalodner, H. A., Carlsten, M., Ellenbogen, P., Bonneau, J. & Narayanan, A. An empirical study of namecoin and lessons for decentralized namespace design. In *14th Annual Workshop on the Economics of Information Security, WEIS 2015, Delft, The Netherlands, 22-23 June, 2015* (2015). URL http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_kalodner.pdf.

[17] of Justice, D. Federal Courts Order Seizure of 82 Website Domains Involved in Selling Counterfeit Goods as Part of DOJ and ICE Cyber Monday Crackdown. URL: https://www.justice.gov/opa/pr/federal-courts-order-seizure-82-website-domains-involved-selling- counterfeit-goods-part-doj (2010). (Accessed November 16, 2017).

[18] S. Wilkinson, J. B. J. P. G. H. P. G. P. H. C. P., T. Boshevski. Storj Whitepaper. URL: https://storj.io/storj.pdf (2016). (Accessed November 15, 2017).

[19] Jaob, A. Deutsche BitTorrent FAQ. URL: http://bittorrent-faq.de/ (2010). (Accessed November 30, 2017).

[20] Labs, P. Filecoin Sale Completed. URL: https://protocol.ai/blog/filecoin-sale-completed/ (2017). (Accessed November 30, 2017).

[21] Dias, D. IPFS - The Permanent Web. URL: https://github.com/ipfs/ipfs (2017). (Accessed November 30, 2017).

[22] Ford, B. Delegative Democracy. URL: http://www.brynosaurus.com/deleg/deleg.pdf (2002). (Accessed November 18, 2017).

[23] Waters, R. Automated company raises equivalent of 120M in digital currency. URL: https://www.cnbc.com/2016/05/17/automated-company-raises-equivalent-of-120-million-in-digital-currency.html (2016). (Accessed November 18, 2017).

[24] Economist, T. The DAO of accrue. URL: https://www.economist.com/news/finance-and-economics/21699159-new-automated-investment-fund-has-attracted-stacks-digital-money-dao (2016). (Accessed November 30, 2017).

[25] Buterin, V. Hard Fork Completed. URL: https://blog.ethereum.org/2016/07/20/hard-fork-completed/ (2017). (Accessed November 21, 2017).

[26] Coindesk.com. Coinbase: Monthly new ICO funding Chart. URL: https://www.coindesk.com/ico-tracker/ (2017). (Accessed November 21, 2017).

[27] Selden S. R., G. M. P. The Shift in Litigation Risks When U.S. Companies Go Public. URL: https://www.transactionadvisors.com/insights/shift-litigation-risks-when-us-companies-go-public (2017). (Accessed November 29, 2017).

[28] Schow, A. Internet gold: Doge + Bitcoin = Dogecoin. URL: http://www.washingtonexaminer.com/internet-gold-doge-bitcoin-dogecoin/article/2541000?custom_click=rss (2013). (Accessed November 29, 2017).

[29] Salvador, R. Jamaican bobsled team boosts value of Dogecoin, currency based on meme. URL: http://www.latimes.com/business/technology/la-fi-tn-jamaican-bobsled-dogecoin-currency-meme-20140120-story.html (2014). (Accessed November 29, 2017).

[30] Kirk, D. How Do I Use Reddits Dogetipbot? URL: http://www.tech-recipes.com/rx/47855/how-do-i-use-reddits-dogetipbot/ (2014). (Accessed November 29, 2017).

[31] random person on the internet, S. Useless Ethereum Token. URL: https://uetoken.com (2017). (Accessed November 21, 2017).

[32] Wiki, E. Ethereum Wiki: Ethash Design Rationale. URL: https://github.com/ethereum/wiki/wiki/Ethash-Design-Rationale (2017). (Accessed November 21, 2017).

[33] Joseph Poon, T. D. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. URL: https://lightning.network/lightning-network-paper.pdf (2016). (Accessed November 30, 2017).

[34] Fyookball, J. Mathematical Proof That the Lightning Network Cannot Be a Decentralized Bitcoin Scaling Solution. URL: https://medium.com/@jonaldfyookball/mathematical-proof-that-the-lightning-network-cannot-be-a-decentralized-bitcoin-scaling-solution-1b8147650800, note = (Accessed November 30, 2017) (2017).

[35] Kronovet, D. Proof of Stake FAQ. URL: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ (2017). (Accessed November 30, 2017).

[36] Norta, A. Self-aware agent-supported contract management on blockchains for legal accountability (2017).

[37] Norta, A. Smart-contracts driven conflict management and resolution for collaborating decentralized autonomous organizations (2017).

[38] Spearpoint, M. A proposed currency system for academic peer review payments using the blockchain technology. *Publications* **5** (2017).

[39] Leiding, B., Memarmoshrefi, P. & Hogrefe, D. Self-managed and blockchain-based vehicular ad-hoc networks 137–140 (2016).

[40] Mccorry, P., Shahandashti, S. F., Clarke, D. & Hao, F. Authenticated key exchange over bitcoin. In *Proceedings of the Second International Conference on Security Standardisation Research - Volume 9497*, SSR 2015, 3–20 (Springer-Verlag New York, Inc., New York, NY, USA, 2015). URL http://dx.doi.org/10.1007/978-3-319-27152-1_1.