Blockchain Land Transfers: Technology, Promises, and Perils

By

Vincent OOI*

SOH Kian Peng**

Jerrold SOH***

Abstract

The blockchain's apparent immutability has attracted significant interest on whether it may be relied on for registering and transferring land. Proponents of blockchain-based land systems point toward data security, automated transacting, and improved accessibility as key benefits; critics raise concerns over structural vulnerabilities, such as majority attacks, and inconsistencies with existing legal frameworks. The literature, however, tends to conceptualise blockchain as one monolithic data structure invariably built on the same mechanisms powering Bitcoin. This paper seeks to situate the debate on a closer understanding of the range of blockchain implementations possible. To this end, we provide a detailed technological survey of established and emerging blockchain technologies, clarifying that different consensus mechanisms, permissioning schemes, and other use-based customisations, are possible. We then re-evaluate the promises and perils of blockchain land transfers in this light, focusing on the English conveyancing system, and illustrate how different implementations involve different advantages and limitations. However, the features necessary to avoid key vulnerabilities also diminish the marginal advantages of using blockchains over traditional electronic databases. Thus, we conclude that blockchains, even properly understood, remain unsuitable for land transfers.

Keywords: Blockchain, Land Registration, e-Conveyancing

A. Introduction

Blockchain technology, though only a decade old, has received much fanfare for its potential to disintermediate fundamental societal processes such as electronic payments and currency

* Lecturer, School of Law, Singapore Management University.

** Adjunct Faculty, School of Law, Singapore Management University.

*** Assistant Professor, School of Law, Singapore Management University. This research is supported by the National Research Foundation, Singapore under its Emerging Areas Research Projects (EARP) Funding Initiative. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not reflect the views of National Research Foundation, Singapore. The authors gratefully acknowledge the support of the Centre for AI and Data Governance, School of Law, Singapore Management University.

exchange. Within the legal sector, there is much hype about the possibility of exploiting blockchain as a secure land register,[1] particularly because of potential cost-savings to consumers and the security features offered by blockchain. Countries that have begun exploring the possibility of blockchain land registries include Sweden, Georgia, Ukraine, Dubai, Brazil, and Ghana.[2] Some countries, like the Netherlands, have gone further in exploring how Artificial Intelligence ("**AI**") can be incorporated with blockchain technology.[3]

Academic literature on blockchain technology may be broadly categorised into four areas.[4] The first includes studies on general legal issues raised by blockchains.[5] The second includes studies on blockchain-based smart contracts and how these can (or cannot) be used to supplement or replace traditional legal contracts like bills of lading.[6] The third focuses on legal and regulatory issues surrounding cryptocurrencies and Initial Coin Offerings.[7] The fourth includes literature discussing issues concerning blockchain land registers and e-conveyancing.[8]

We begin by first delving into the specifics of how blockchains work in Part B, from which we draw out some general features of blockchain systems. From this, we identify the features needed to negate the key vulnerabilities of blockchain which diminish any marginal advantages of using blockchain over traditional electronic databases. The whole process of conveyancing and land registration is canvassed in Part C. While we will focus on the English system, many of the features set out in this part will be recognisable across the common law world – for instance, the central role the Land Registry plays in the conveyancing process. This sets the stage for an analysis of the advantages and disadvantages of using blockchain in land

---

1 See e.g. Rod Thomas, 'Blockchain's incompatibility for use as a land registry: issues of definition, feasibility and risk' (2017) 6(3) EPLJ 361.

2 Rohan Bennett, Mark Pickering and Jason Sargent, 'Transformations, Transitions, or Tall Tales? A Global Review of the Uptake and Impact of NoSQL, Blockchain, and Big Data Analytics on the Land Administration Sector' (2019) 83 Land Use Policy 435, 440-441.

3 Jan Veuger, 'Dutch Blockchain, Real Estate and Land Registration' (2020) 12(2) Journal of Property, Planning and Environmental Law 93-108.

4 Karen Yarbrough and John Mirkovic, 'Blockchain Pilot Program Final Report' (Cook County Recorder of Deeds, 2017) <http://cookrecorder.com/wp-content/uploads/2016/11/Final-Report-CCRD-Blockchain-Pilot-Program-for-web.pdf> accessed 7 January 2021; Jacques Vos, 'Blockchain-Based Land Registry: Panacea, Illusion Or Something In Between?' (2017) European Land Registry Association; and Nogueroles Peiro and Martinez Garcia, 'Blockchain and Land Registration Systems' (2017) 6(3) EPLJ 296.

5 Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (2015) <https://ssrn.com/abstract=2580664> accessed 7 January 2021; Jean Bacon, Johan Michels, Christopher Millard and Jatinder Singh, 'Blockchain Demystified' (2017) <https://ssrn.com/abstract=3091218> accessed 7 January 2021; Christopher Millard, 'Blockchain and Law: Incompatible Codes?' (2018) 34(4) Computer Law & Security Review 843; and Edmund Schuster, 'Cloud Crypto Land' (2020) Modern Law Review 1.

6 Eliza Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (2017) 9(2) Law, Innovation and Technology 269.

7 Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80(6) MLR 1073; Matteo Solinas, 'Bitcoiners in Wonderland: Lessons from the Cheshire Cat' (2019) LMCLQ 433; and Oonagh McDonald, 'Regulating Crypto Assets' (2020) 41(11) Company Lawyer 335.

8 Thomas (n 1); Rod Thomas and Charlie Huang, 'Blockchain, the Borg Collective and Digitalisation of Land Registries' (2017) Conv 14; Victoria Lemieux, 'Trusting Records: Is Blockchain Technology the Answer?' (2016) 26(2) Records Management Journal 110; and Alvin See, 'Blockchain In Land Administration? Overlooked Details In Translating Theory Into Practice' in Gary Chan and Yip Man (eds) *AI Data and Private Law* (Hart Publishing, 2021).

registration in Part D. Insofar as the development of land registries to accommodate new technologies are concerned, there are four discernible stages: 1) traditional land registry, 2) online land registry, 3) distributed ledger technology ("**DLT**") registry and 4) systems building on DLT (involving the use of smart contracts and AI). We argue, based on the foregoing discussion in Parts B and C, that given the serious concerns with using a public blockchain model, only a private blockchain is feasible for use where land registries are concerned. However, even a private blockchain may not be worth adopting for two reasons. First, the security offered by private blockchains is already realisable through an electronic land registry where access is limited to authorised users. Second, blockchain is merely an alternative form of data storage that also suffers from the same inherent limitations faced by any land registry, *viz*, that no land registry can ever be a complete repository of information relating to land.

In summary, the hype over using blockchain in land registration has obscured the key question of what advantage blockchain actually offers over a non-DLT digitised land registry. We submit that the real advantages DLT offers stems from digitisation, and not from the features of DLT *per se*. Therefore, the goal should be to digitise land registries instead of jumping aboard the blockchain bandwagon.

B. The Technology

We begin by explaining the underlying technology behind blockchain. This section provides a basic understanding of the technology underlying blockchain, on which we build our analysis in Part D, and will cover three areas: (a) a broad overview and origins of blockchain, (b) its core features and (c) possible customisations.

The blockchain is an algorithm proposed by the pseudonymous Satoshi Nakamoto in 2008.[9] While much subsequent literature has explored the uses and implications of blockchain technology in wide-ranging areas, including for the law, Nakamoto's original conception of the blockchain was more specific. To Nakamoto, blockchain represented "a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions".[10]

Nakamoto's concise description of blockchain's foundational purpose is worth unpacking. First, the "double-spend problem" refers to the problem transacting parties face in verifying that the counterparty has not already spent the consideration he purports to furnish. In a world without trust or trusted intermediaries, ensuring that the counterparty has, and can give, what he claims to have would involve significant transaction and information costs that render the otherwise mutually beneficial transactions unfeasible.[11]

---

9 Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) <https://bitcoin.org/bitcoin.pdf> accessed 7 January 2021.

10 ibid.

11 ibid.

Second, a "peer-to-peer distributed timestamp server" broadly refers to a network of computers that are connected to each other and all partake in establishing the current state of the network. "Distributed" simply means data records are stored across multiple computers and organisations rather than "centralised" in one.[12]

Third, this distributed server is meant to provide "computational proof" for transactions.[13] This means that sufficiently conclusive evidence for the authenticity of blockchain transactions is to come from computerised, mathematical, and indeed cryptographic algorithms. Schemes of proof used in blockchain will be elaborated upon below.

Fourth, the objects to be proven are "transactions" which Nakamoto defines as transfers of "electronic coins".[14] In turn, such coins comprise nothing more than "a chain of digital signatures" that carry information about previous transactions relating to the coin, the digital identity of the present owner, and a cryptographic lock tied to the present owner.[15] This lock ensures that only the present owner who holds the matching key may spend the coin. To transfer the coin, the present owner first unlocks the coin using his key. He then "changes the locks" by appending the cryptographic lock tied to the intended payee onto the coin instead. Other information necessary to the transfer protocol is also added to the coin. He then broadcasts the prepared package of information to the distributed server for completion.

After the transaction is broadcast and assuming the transaction is valid, others on the distributed server pick up and include the proposed transaction into a putative block yet to be added to the ledger. A protocol known as a "consensus mechanism" is then followed to ascertain if particular code-enforced requirements are fulfilled before the block and its transactions can be appended to the ledger. It is only then that the transactions are finalized and completed or, in blockchain parlance, become "immutable".[16]

Consensus mechanisms will be elaborated upon below. For present purposes, the crucial point is that the blockchain, as originally conceived, was specifically meant to facilitate a verifiable yet intermediary-free electronic payment system by solving the "double-spend" problem without recourse to trusted central authorities. Further, such a payment system involves the secure transfer of packages of information regarding each coin's ownership and transactional history.

Core Features

In this light, this article defines "core" features of the blockchain as those necessary to solve the double spend problem in the absence of trusted intermediaries. These are the technical

[12] Bacon, *et. al.* (n 5).
[13] Nakamoto (n 9).
[14] ibid.
[15] ibid.
[16] Immutability does not equate to being tamper-proof. It is only that records are tamper-evident. See Bacon, *et. al.* (n 5); Millard (n 5).

features which give rise to the three *indicia* of blockchain-type databases identified by Thomas.[17]

(1) Blocks

Blocks are a packaged unit of information. Minimally, each block must contain cryptographic information and meta data that allow them to be chained together securely. This is explained in greater detail in the subsequent discussion on chains. Other than this, there is no theoretical limit to the data which blocks can store. Any information that can be stored in computer memory could potentially be packaged into a block. Traditionally and most commonly, blocks are used to store transaction records, as in the Bitcoin protocol. However, the Ethereum protocol allows blocks to contain executable computer code, making it possible for parties to write computerised instructions onto the blockchain that cannot later be altered.[18] The literature knows these as "smart contracts", though the representativeness of this label is contestable.[19] Significantly, the Ethereum protocol which hosts these contracts claims to provide a Turing-complete programming language.[20] This means that the programming language powering Ethereum can encode any computable function, including infinite loops. It is thus theoretically possible to program a new cryptocurrency on the Ethereum blockchain itself. This is in fact how tokens in Initial Coin Offerings are typically issued.[21]

(2) Consensus Mechanisms

On their own, blocks are simply packets of data. A list or matrix of blocks would thus be no different from a traditional database. The second feature necessary for a blockchain to address the double-spend problem lies in the use of an algorithm — an agreed process, broadly speaking — for verifying transaction records.[22] These processes are more formally known as "consensus mechanisms".[23]

Consensus mechanisms are typically built on cryptographic hash functions. A "hash function" is a formula for converting a given input into a definite output.[24] A cryptographic

[17] Thomas (n 1). These three indicia are: a) trustless transactions, b) durability and c) transparency and immutability.

[18] Vitalik Buterin, 'A Next-Generation Smart Contract and Decentralized Application Platform' (23 Jun 2020), <https://github.com/ethereum/wiki/wiki/White-Paper> accessed 7 January 2021.

[19] Mik (n 6).

[20] Buterin (n 18).

[21] Anthony Nolan, Edward Dartley, Mary Baker, John ReVeal and Judith Rinearson, 'Initial Coin Offerings: Key US Legal Considerations for ICO Investors and Sponsors' (2018) 19(1) Journal of Investment Compliance, 1-9.

[22] Millard (n 5).

[23] Christian Cachin and Marko Vukolić, 'Blockchain Consensus Protocols in the Wild' in Andrea Richa (ed), *31st Intl. Symposium on Distributed Computing* (DISC, 2017); Wenbo Wang, *et. al.*, 'A Survey on Consensus Mechanisms and Mining Management in Blockchain Networks' (2019) 7 IEEE Access; and Millard (n 5).

[24] An example is a formula that converts each alphabet into its alphabetical index. 'A' is converted to 1, 'B' is converted to 2, 'C' to 3 and so on. Applying this formula, the input 'ABC' would be converted, or 'hashed', to '123'. A critical feature for a workable hash function is that a given input is always hashed into the same output. This allows the hash function output to preserve the information contained in the original input, albeit in a different form. For contrast, suppose that each alphabet is not mapped to a certain number but an arbitrary

hash function is a one-way hash function. "One-way" means that given an arbitrary input-output pair, although it is possible to verify whether the input indeed produces that output, the converse is not true: given the output, it is impossible or at least prohibitively costly to uncover the original input.[25] A well-known cryptographic hash function is the SHA-256 function used by Bitcoin. Consider the following output from SHA-256:

ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1

Even if the original input data that produced the above was made public, it would be difficult to reverse engineer the input data from the string of seemingly random alphabets and digits above.[26] It then becomes possible to use the phrase for encryption purposes.

Cryptographic hash functions are instrumental to how consensus mechanisms allow transactions to be verified and securely added to the blockchain without recourse to trusted central authorities. This is best illustrated with an example. The original consensus mechanism proposed by Nakamoto (often referred to as "**Nakamoto consensus**") and used by the Bitcoin protocol is the "Proof-of-Work" ("**POW**") scheme. Before a new block can be added to the chain, all transactions in the block, as well as a string representing the current time, are aggregated into a long, continuous string. For the block to be confirmed and its transactions executed, an integer must be found that, when appended to the combined string and hashed, yields a hashed output that begins with a certain number of zeroes.[27] To illustrate, suppose a block has only one transaction, being "Transfer 1 coin from user 1 to user 2", and the present time is the 1st of January, 2011 at 1111 hours. For this block to be accepted, an integer *X* must be found such that, the following string (hereinafter the "**solve string**"):

"Transfer 1 coin from user 1 to user 2 2011-1-1-1111 *X*"

when hashed through SHA-256, yields an output such as

"00000e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1"

The party who finds the right *X* is said to have "solved" or "mined" the block. Because SHA-256 yields cryptographic outputs, if an hour later an attacker modified the transaction to read "Transfer 2 coins from user 1 to user 2" instead, the attacker would have to expend considerable effort to find a new integer *Y* such that "Transfer 2 coins from user 1 to user 2 2011-1-1-1211 *Y*" hashes to an output with the requisite number of leading zeroes. Individual blocks are thus resistant to tampering.

---

one. Even with both the input and output (say, 'A' and 36), it would be impossible to tell whether the output originated from the input.

25 Bacon, *et. al.* (n 5).

26 The input data used to produce the above output was 'blockchain'.

27 Nakamoto (n 9).

<u>(3) Chains</u>

Tampering with historical records (i.e. previous blocks) is made even more difficult by chaining: for every new block, the hash of the *previous* block is included in the solve string. If an attacker modified a transaction in the first block, the hash associated with that block would be altered as well. Thus, when the first block's hash changes, so does the second block's solve string. The hash associated with the second block would change as well. The attacker would then have to solve every block subsequent to the block he modified in order to falsify any one transaction.

Because the Bitcoin protocol only accepts the longest blockchain as the "true" record, the attacker must not only be able to solve every subsequent block in the chain – he must do so faster than all other miners so that he creates a chain longer than the current consensus. By modelling block completion as a Poisson process, Nakamoto showed that the probability of a successful attack decreases quickly to zero over time.[28] That is, unless the attacker commandeers more than half of the total computing power amongst all miners. If so, he may be able to out-compute the current longest chain. This is known as a "51 percent attack".[29]

Although the "chain" metaphor evokes the image of a linear series of blocks arranged in chronological fashion, it is not necessary for blocks to be connected this way. New types of blockchain architectures have been proposed and implemented that store blocks within graph structures.[30]

<u>(4) Identification Mechanism</u>

A robust consensus chain could still be undermined if parties can masquerade as others to propose or validate transactions. Blockchain systems thus typically use public key cryptography to verify participants' identities. This differs from the cryptographic hash functions earlier explained. Recall that SHA-256 generates one cryptographic output from one data input. Public key cryptography functions generate two asymmetric constructs. The first is the "public key", which analogises to a lock in that, although the public key affords entry only to those holding the right corresponding key, the lock itself is visible and can be scrutinised by the public. The second is the "private key", which is more like an actual physical key.

Each private-public key pair matches uniquely and exclusively, so only the private key holder may authenticate into anything behind the public key lock.[31] In blockchains generally, records owned by the relevant party are secured by that party's public key and may only be accessed using that party's private key.[32] Notice that "identification" in the blockchain sense is not tied to any party's personal details. The only concern is whether that party holds the right

---

[28] ibid.

[29] For details on this sort of attack see Part D.

[30] Patrick Schueffel, 'Alternative Distributed Ledger Technologies Blockchain vs. Tangle vs. Hashgraph - A High-Level Overview and Comparison' (2017) <https://ssrn.com/abstract=3144241> accessed 7 January 2021.

[31] In actual implementation, a challenge-response system is used. See Bacon *et. al.* (n 5).

[32] Bacon, *et. al.* (n 5).

private key. Bitcoins can thus be stolen if their corresponding private keys are stolen.[33] One would also observe that from this that without the private key, parties cannot change any records on the blockchain behind the private key lock. As we will discuss below, this has implications for a blockchain land register.

Variable Features

Blockchain's core features are in turn supported by auxiliary features that are generally speaking neither new concepts nor necessary for ensuring the blockchain's tamper-resistance quality. Depending on what blockchain is sought to be used for, these features can be customised accordingly.

Type of Consensus Mechanism

While every blockchain needs a consensus mechanism, POW is not the only possible one. Computer science literature is replete with proposed alternatives that are too many in number and variation (and too fast-evolving) to enumerate here.[34] This paper will briefly outline the two key categories of alternative consensus mechanisms.

Proof-of-Stake

POW secures the blockchain's integrity by making falsifying transactions very hard work. This is however double-edged because the computations required to validate Bitcoin transactions leads to high computational and electricity costs.[35] The time necessary to solve the cryptographic puzzle each time also leads to slow transaction rates.

Proof-of-stake ("**POS**") mechanisms were proposed as a less computationally-expensive alternative. In POS schemes generally, blocks are mined by a process roughly similar to a weighted shareholders' vote. That is, "the influence an agent has is proportional to the number of coins (or "stake") it holds".[36] For example, under the Casper POS protocol proposed to be used by Ethereum, parties who want to participate in validating transactions (known as "validators") must first put up a certain amount of cryptocurrency as deposit. Every 100th block in the chain is a designated "checkpoint" that requires two consecutive passing votes to be finalized onto the blockchain. First, a putative checkpoint is "justified" if (a) it is linked to a previously justified block, and (b) a supermajority of two-thirds of the validators' voting power (measured by deposit amount) votes in favour of the checkpoint. Second, the (now) justified

[33] Kelvin Low and Ernie Teo, 'Legal Risks of Owning Cryptocurrencies' in David Lee and Robert Deng (eds), *Handbook of Blockchain, Digital Finance and Inclusion* (Elsevier, 2018).

[34] For a comprehensive explanation and evaluation of consensus mechanisms in blockchain see Cachin and Vukolić (n 23); and Wang, *et. al.* (n 23).

[35] Buterin (n 18).

[36] Vitalik Buterin and Virgil Griffith, 'Casper the Friendly Finality Gadget' (25 October 2017) <https://arxiv.org/abs/1710.09437> accessed 7 January 2021.

checkpoint is "finalised" and added to the chain if a checkpoint subsequently linked to it becomes justified (i.e. a supermajority also votes in favour of the next checkpoint).[37]

To deter errant voting behaviour, validators who violate either one of two "slashing conditions" will have their deposit forfeited.[38] Buterin proved by contradiction that under these constraints, no two conflicting transaction checkpoints can be finalised onto the chain unless more than one-third of the voting power violates a slashing condition and thus forfeits their deposits.[39]

This approach remains susceptible to attackers who care not for their deposits but command at least one-third of the total voting rights. However, not all POS mechanisms are implemented identically. Other mechanisms may, for example, randomly assign the right to validate a transaction block with those that have higher stake in the relevant cryptocurrency having a greater chance to be chosen.[40] The key principle is that POS discourages transaction falsification in two ways. First, validation rights are limited to those with some stake in the system. The assumption is that those with higher stakes in the system are disincentivised from taking actions which may significantly undermine the cryptocurrency's value.[41] Second, for the Casper protocol especially, errant behaviour is financially penalised by deposit forfeiture.

It is noteworthy here how blockchain implementations may rely not only on code-enforced obstacles for attackers, but economic disincentives as well. These economic disincentives are feasible for cryptocurrencies because much of any value in a currency as virtual and intangible as Ethereum stems from parties' trust in the underlying protocol. A validator who undermines this trust in order to secure more Ethereum achieves a pyrrhic gain if the price of the cryptocurrency crashes as a result.

It may seem at first that this has little application where real property is involved, since the value of land ownership rights on a hypothetical blockchain land register will remain unchanged. However, once the trust in the system has been eroded, it is highly likely that the relevant authorities will stop recognising the system and revert to the prior method of land registration.

<u>Byzantine Fault Tolerance</u>

Both POS and POW operate on the basis that something must be proven by some party before a transaction can be finalised onto the chain and executed. The blockchain literature now refers to these schemes generally as "proof of X" ("POX") mechanisms.[42] A different family of

---

37 ibid.
38 The slashing conditions are that (a) a validator must not vote simultaneously for two blocks at the same target height and (b) a validator must not vote within the span of its other votes.
39 Buterin and Griffith (n 36).
40 Iddo Bentov, Charles Lee, Alex Mizrahi and Meni Rosenfeld, 'Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake' (2014) 42 ACM SIGMETRICS Performance Evaluation Review 34.
41 Buterin and Griffith (n 36).
42 Wang, *et. al.* (n 23).

consensus mechanisms rely on the Byzantine Fault Tolerance ("**BFT**") algorithm which pre-dates blockchain.[43]

The algorithm gets its name from how it was designed to solve Lamport, Shostak, and Pease's Byzantine Generals' Problem.[44] To state the problem simply, the question is how multiple parties may coordinate and agree on one course of action despite the presence of "faulty" parties who may send false or malicious signals, and whose "faulty" status is not known. BFT uses a recursive broadcast and voting process to overcome this problem.[45] Castro and Liskov showed that this technique guarantees that the correct transaction will be agreed upon and recorded even if there are faulty entities, but only provided that less than or equal to one-third of the entities in the network are faulty.[46]

Therefore, BFT based methods are generally susceptible to attackers who command more than a certain number of on-chain entities. This should be distinguished from the vulnerabilities inherent in POW (where the critical resource is computing power available), and POS (where the critical resource is the attacker's stake and willingness to forsake the same). In any case, the important point to note is that the blockchain does have its vulnerabilities, and as we argue in Part D, these very vulnerabilities and the solutions may well negate any potential benefits a blockchain land register may have.

<u>Permissioning</u>

As with traditional databases, blockchains allowing different permission levels may be set for different user roles. In blockchains, of course, the right to write, alter, or delete data is dictated by consensus. Nonetheless, other rights not central to blockchain's tamper-resistance can still be tuned to purpose. Bacon and others thus note that "blockchain technology can be applied in various ways to create platforms with different features, including with regard to: 1) who can propose new transactions to be added to the ledger; 2) who stores a copy of the ledger; 3) who can add new blocks to the ledger; 4) who can view the ledger; 5) whether users are identifiable; and, 6) who controls the platform's underlying software".[47]

---

[43] Miguel Castro and Barbara Liskov, 'Practical Byzantine Fault Tolerance and Proactive Recovery' (2002) 20 ACM Transactions on Computer Systems 398.

[44] Leslie Lamport, Robert Shostak and Marshall Pease, 'The Byzantine Generals Problem' (1982) 4 ACM Transactions on Programing Languages and Systems 382.

[45] Castro and Liskov (n 43). To briefly outline the algorithm's contours: when a transaction is proposed, every on-chain entity will repeat the proposed transaction out loud to the rest of the on-chain entities and cite the entire provenance of where the entity heard this from. This continues for a number of rounds (with the provenance list getting longer each time) depending on the number of faulty entities anticipated to be within the network. By the end of this process each entity will have heard numerous suggestions of what the proposed transaction is and the sources so claiming. Provenance trails that have passed through faulty entities would suggest false transactions while provenance trails that have passed through only non-faulty entities would bear the 'true' transaction. A series of majority votes are then conducted to select the transaction to prefer at each majority round, starting from suggestions received at the final round. The result of each round's vote is then escalated as the vote for each previous round. The vote-and-escalate process continues until the first round of repetition which also represents the final vote. The final vote determines the transaction that is ultimately recorded.

[46] Castro and Liskov (n 43).

[47] Bacon, *et. al.* (n 5).

Additionally, as we have seen with POS-type protocols, rights to participate in the consensus process may also vary. Permissions to specific participants are not necessarily set in stone. In Ethereum Casper, the group of recognised validators changes over time as users post and withdraw deposits. In Nakamoto consensus, anyone may participate in the mining process, but only the first miner to solve the cryptographic puzzle may add a new block. Who solves the puzzle first can differ each time. In these cases, it is the *procedural mechanism for assigning permissions* that stays the same. This is in turn controlled by the developers who control the protocol's underlying software.

Private and Public Chains

To whom what permissions are granted in turn determine whether a blockchain may be termed a "public" or "private" chain. Blockchains are "public" if anyone may, by installing the relevant software, acquire rights to view records, transact, and participate in the consensus process.[48] Bitcoin and Ethereum are both examples of public blockchains. Conversely, chains that limit viewing, transacting, and/or consensus rights to certain entities or group of entities are "private" chains. It should be noted that the public-private divide here is continuous rather than binary. One private chain may allow public viewing of its records, but only allow certain organisations to vote on consensus. Another may limit transaction rights to one or two central authorities.

Whether a blockchain is private or public has real implications for data integrity because of the way consensus mechanisms work. It is much easier to launch a 51% attack on a private chain comprising only ten entities than an equivalent public chain subscribed to by thousands. For this reason, private chains are typically permissioned and rely on BFT consensus where consensus rights are limited to parties least likely to be faulty, while public chains are typically permissionless and rely on proof-of-concept mechanisms.[49]

There is however a practical limit to how permissioned or private a blockchain can get. Recall that the blockchain's foundational purpose is to guarantee trust in the absence of a trusted central authority, such as the government, or in our case, the Land Registrar. A private chain where all consensus rights are centralised within one organisation defeats this very purpose. One may ask if another database type should have been used instead.

Two points emerge from the preceding. First, the blockchain comes in different, somewhat customisable, flavours. It is not one fixed data structure, but a family of possible data structures that can involve different consensus mechanisms, permissioning, etc. A full treatment of whether blockchain can or should be used in land registration (and, it is suggested, for any legal purpose) cannot therefore limit itself to considering specific implementations of the blockchain. The disadvantages of a blockchain land register should be considered bearing in mind that certain issues may be alleviated or solved by a different implementation.

[48] Dominique Guegan, 'Public Blockchain versus Private blockhain' (18 May 2017) CES Working Paper 2017.20, 2 <https://halshs.archives-ouvertes.fr/halshs-01524440> accessed 7 January 2021.

[49] Cachin and Vukolić (n 23).

Second, the blockchain was originally conceived, and indeed still serves, as a way to store data. Although the distributed way in which the blockchain does this distinguishes it from traditional databases, the trite principle that every data structure involves a trade-off applies equally to the blockchain.[50] How the Nakamoto consensus trades-off high computational costs and slower transaction rates in order to achieve tamper-resistance has already been canvassed. The proposed advantages of a blockchain land register should be considered with this in mind. The relevant comparison to make is not between a blockchain-based system and whatever system currently in place, but a between blockchain-based system and other electronic land registers built on alternative, and perhaps "conventional" databases.

With these two points in mind, this paper now proceeds to consider the conveyancing and land registration system.

C. How Conveyancing and Land Registration Works

In this section, to motivate our discussion on how blockchain can be customised for land transfers, we lay out in broad strokes how conveyancing and land registration works in England. We note that while our focus is on England's land registration system, our observations could apply to other systems (e.g. The Torrens system). A typical transaction involving the sale and disposition of registered land from one party (the "seller" or his solicitors) to another (the "buyer" or his solicitors) can be simplified into five distinct stages: 1) pre-contract stage; 2) contract stage; 3) post-contract and pre-completion stage; 4) completion stage, and 5) post-completion stage.

(1) Pre-Contract Stage

The buyer and seller will first negotiate the terms of the contract of sale. As part of the process, the seller will usually show some evidence that he has title to the land and that he is entitled to sell the interest in the land to the buyer. This evidence will invariably be in the form of an "official copy" of the registered title obtained from Her Majesty's Land Registry (the "**Land Registry**").[51] The official copy will reveal, *inter alia*, the description of the land, the title number, the class of title, the identity of the registered proprietor, and whether there are encumbrances on the land.[52]

Generally, the principle *caveat emptor* applies.[53] Thus, the buyer will usually conduct further searches and enquiries on the land. Such searches include an official search with priority protection which will (a) confirm that the information given to the buyer is accurate, and (b)

---

[50] Allan Borodin, 'Computing (and Life) Is All about Tradeoffs' in Andrej Brodnik, Venkatesh Raman, Alfredo Viola and Alejandro López-Ortiz (eds), *Space-Efficient Data Structures, Streams, and Algorithms: Papers in Honor of J. Ian Munro on the Occasion of His 66th Birthday* (Lecture Notes in Computer Science, Springer 2013).

[51] Elizabeth Cooke, Stuart Bridge and Martin Dixon, *Megarry and Wade: The Law of Real Property* (9th edn, Sweet & Maxwell 2019), para 6–120.

[52] ibid.

[53] Cooke, *et. al.* (n 51), para 14–069.

ensure that no entry can be made on the register during the priority period.[54] If the buyer requires further proof of the seller's title, he will stipulate this in the contract of sale.[55]

<u>(2) Contract Stage</u>

Once the buyer and seller are satisfied with the results of their negotiation and due diligence, copies of the contract of sale will be prepared, signed and exchanged. Depending on the terms of the contract, the buyer may have to pay a deposit upfront which also acts as part payment of the purchase price.[56] The buyer may also choose to lodge a notice with the registrar so as to protect his interest under the contract of sale,[57] although an official search with priority protection would generally be sufficient to protect his interest.[58]

<u>(3) Post-Contract and Pre-Completion Stage</u>

After the contract of sale has been executed, a form of transfer will be prepared in the manner stipulated by the Land Registry.[59] This form of transfer will be executed by the seller as a deed at the completion stage.[60] The buyer will also carry out pre-completion searches and enquiries so as to confirm that the information received by him thus far remains accurate.

<u>(4) Completion Stage</u>

At the date of completion, the buyer will transfer the balance of the purchase price to the seller. Upon receipt of the funds, the seller will send to the buyer the signed deed of transfer and other documents required under the contract of sale. If the buyer is funding the purchase by way of a mortgage, the mortgage will be simultaneously completed with the foregoing steps. In higher value transactions, the buyer and seller may decide to complete the sale and disposition of the land via an escrow agent.

<u>(5) Post-Completion Stage</u>

After completion, the seller will have to deal with the discharge of his mortgage, if any.[61] The buyer will have to pay the relevant stamp duty land tax[62] and register his title with the Land Registry.[63] Prior to the registration of the buyer's title, the seller remains the legal owner of the land. After the buyer registers his title, he will become the legal owner of the land. While there were some concerns over the hiatus between the date of making the disposition of the land and the date of its registration (i.e. the registration gap), such concerns are less significant today

54 ibid, para 14–085.
55 ibid, para 6–148.
56 ibid, para 14–048.
57 ibid, paras 6–073, 6–074, and 6–147; and Land Registration Act 2002, pt 4.
58 ibid, para 6–147.
59 ibid, para 6–149.
60 ibid; and Land Registration Rules 2003, sch 9.
61 ibid, paras 24-101 and 24-102.
62 Finance Act 2003, pt 4.
63 Cooke, *et. al.* (n 51), para 6-150.

due to priority protection, judicial developments and the proposed re-introduction of electronic conveyancing.[64]

The stages set out above provide a general overview of the conveyancing process. There are of course other forms of contracts for the sale or disposition of land, such as, for example, an option to purchase or a right of pre-emption.[65] Land could also be conveyed to another party for no consideration (i.e. a gift). However, our focus is on the functions of the Land Registry within the conveyancing process described above. The Registrar maintains two registers: the register of title and the register of cautions against first registration. The latter enables a person claiming an interest in unregistered land to be notified of any application for the first registration of that land, allowing him to object to registration unless his rights are appropriately protected in the register.[66] The register of title is now typically kept in digital form.[67] There are three parts to each individual register; a) property register, b) proprietorship register and c) charges register. The first contains a description of the registered estate and other details (such as easements). The second records, *inter alia*, details of the class of title, name of the registered proprietor, an address for service. The third is a record of incumbrances such as registered charges and interests protected by notice. This article will therefore examine the advantages and disadvantages of employing a DLT-based land register in that context.

D. Re-considering the Promises and Perils of Blockchain Land Transfers

As alluded to in Part B above, the structure and design of the *specific* blockchain system adopted for land registration – for example, whether the blockchain is public, private, or a hybrid – would naturally have its associated advantages and disadvantages.[68] In this section, we demonstrate that a clearer understanding of blockchain technology qualifies seven points about the promises and perils of blockchain land transfers, and that overall, most, if not all of the advantages gainsaid by a private blockchain model, which is by far the most ideal model for a land registry, can already be realised through a digital land registry.

(1) Data Transparency

In blockchain systems, land can be represented by digital addresses which contain information relating to, *inter alia*, occupancy rate and legal status. Malviya argues that this would increase data transparency and remove the information asymmetry advantage possessed by brokers.[69] It is also possible to integrate data held by multiple government departments onto the digital

---

64 ibid, para 6-150.
65 ibid, para 14-002.
66 ibid, para 6-044.
67 ibid, para 6-113.
68 Jacob Vos, Christiaan Lemmen and Bert Beentjes, 'Blockchain-based Land Administration: Feasible, Illusory or a Panacea?' (World Bank Conference on Land and Poverty, Washington DC, 2017).
69 Hitesh Malviya, 'Blockchain for Commercial Real Estate' (2017) <https://ssrn.com/abstract=2922695> accessed 7 January 2021.

addresses of land:[70] instead of sending separate legal requisitions to different government departments, relevant information can be automatically synced into the digital addresses of land. Thus, blockchain systems would increase the accessibility of information to the masses and accelerate the due diligence aspects of the conveyancing process.

However, it is noted that data transparency is not unique to blockchain systems: an electronic conveyancing system has the ability to perform the same function.[71] In addition, even if it is accepted that it is beneficial for information to be readily accessible to the masses, at least two further points may be raised. First, the content information stored on blockchain may not be easily understood. Second, not all information would be reflected in the digital addresses, e.g. unregistered overriding interests.[72] Therefore, licensed professionals and lawyers might still be needed to advise on the information available and to conduct due diligence. In this regard, the extent of time saved may not be as significant as it appears.

<u>(2) Expediting Transactions</u>

In a typical conveyancing process, the seller will only send the signed purchase deed to the buyer when it receives the purchase money. There is a risk that the seller would, upon receiving the money, refuse to transfer the signed purchase deed. To protect the buyer against this risk, parties to a typical sale and disposition of land may sometimes choose to appoint an escrow agent to assist completion.

In a blockchain land registration system, a peer-to-peer ("**P2P**") exchange platform can be built so as to facilitate the transfer of tokens representing the land (the "**land token**").[73] Under such an exchange platform, prospective sellers can list their land tokens and their terms of sale, and prospective buyers can purchase those land tokens in exchange for money. Malviya suggests that this would eliminate the need for, *inter alia*, escrow agents, thereby reducing the speed of transaction from weeks to "minutes or seconds".[74] In addition to eliminating middlemen, the exchange platform has the potential to erase the need for multiple steps in the conveyancing process. For example, buyers would no longer need to register their title post-completion as the land token would be sufficient proof of ownership. This would also have the effect of eliminating the "registration gap", and the priority of the interest would be determined by the transfer of the land token.

Furthermore, where smart contracts are integrated into a blockchain system or its exchange platform, certain events could be programmed to trigger automatically upon the fulfilment of a set of criteria.[75] For example, the seller's mortgagee could be automatically paid, and the seller's mortgage simultaneously discharged, upon the exchange of the seller's land token for the buyer's money. Stamp duty land tax could also be automatically calculated,

---

70 Yarbrough and Mirkovic (n 4).
71 See Gabriel Brennan, *The Impact of eConveyancing on Title Registration: A Risk Assessment* (1st edn, Springer 2015), 74–86.
72 Land Registration Act 2002, s 29(2)(a)(ii); and Schedule 3 to the Land Registration Act 2002.
73 Malviya (n 69).
74 ibid.
75 ibid; see also Vos *et. al.* (n 68) 16.

charged, and transferred to Her Majesty's Revenue and Customs during the exchange of land tokens. The effect of automation is that land transactions would be expedited to a significant extent.

That said, there are hurdles to using smart contracts in land transactions. Land transactions are complex, and while some might argue that machine learning may be used to optimise land transactions,[76] it still does not resolve the problem of having to determine the intentions of parties, but adds to the complexity of ascertaining such intention when AI is involved.[77] This leads us to another potential issue in using smart contracts to optimise land transactions. Recall that smart contracts are less contracts than simply computer code stored on the blockchain.[78] The point at which contractual events are triggered may not always be reducible to computer code; even if it is, an interface between the code and the real world is necessary to capture the trigger event within the code. To illustrate, completion could be subject to the buyer's right to rescind the contract in the event that the property differs "substantially" from what he had been led to expect.[79] It could also be subject to "satisfactory" replies to legal requisitions. Legal terms such as "substantially", "satisfactory" and "reasonably" are arguably difficult to translate into smart contracts because they rely on fuzzy rather than formal or Boolean logic. Thus, if smart contracts are used, they must be sufficiently flexible to accommodate these terms,[80] and disputes arising from them must be amenable to resolution (whether by the code protocol itself or more conventional legal processes). It is therefore not immediately clear whether utilising a blockchain land registry to enable optimisation of land transactions through smart contracts has immediate benefits.

(3) Accessibility of Land

Another advantage of a peer-to-peer exchange platform built over a blockchain land registration system is that land would be easily tradeable like equities. In fact, the flexibility provided by a blockchain system permits property ownership in multifarious forms. This could, for instance, be accomplished through sidechains which are essentially secondary blockchains connected to the main blockchain.[81] Assets stored on the main blockchain can be transferred to and from the sidechain at a fixed or predetermined exchange rate.[82] Vos and others suggest that, with sidechains, it is possible to divide a large property into smaller units, each of which

76 Andrew Saull and Andrew Baum, 'The Future of Real Estate Transactions' (2019) University of Oxford Research, Saïd Business School < https://www.sbs.ox.ac.uk/sites/default/files/2019-03/FoRET-ReportFull_1.pdf> accessed 7 January 2021 at 41 – 45.

77 See Vincent Ooi, 'Contracts Formed by Software: An Approach from the Law of Mistake' (2022) Journal of Business Law 97.

78 Kelvin Low and Eliza Mik, 'Pause the Blockchain Legal Revolution' (2020) 69 ICLQ 135, 166. Low and Mik point out that smart contracts are not contracts in the legal sense although nothing stands in the way of them having legal effects).

79 See e.g. the *Law Society's Standard Conditions of Sale* (Fifth Edition – 2018 Revision), cl 7.1.1.

80 But see Jeremy Sklaroff, 'Smart Contracts and the Cost of Inflexibility' (2017) University of Pennsylvania Law Review 263, 291-296.

81 Amritraj Singh, *et. al.*, 'Sidechain Technologies in Blockchain Networks: An examination and State-of-the-Art Review' (2020) Journal of Network and Computer Applications, 2.

82 ibid.

can be traded with others (the owners of such units may be referred to as "unitholders").[83] This might have the effect of increasing levels of property ownership, through greater accessibility of land.

However, lowering barriers to property ownership in this fashion may encourage speculation or introduce short-term uncertainty to the property market.[84] This would be an important consideration for policymakers given its potential to drive up property prices, thereby making it harder for people to own property. Currently, some of the largest barriers to home ownership include, *inter alia*, raising deposits and obtaining a mortgage.[85] It is difficult to see how having a peer-to-peer exchange platform running off a blockchain land registry can help reduce some of these barriers for homeowners.

Such an exchange platform may also require an overhaul of existing laws, *viz*, financial and securities regulations. For instance, industry standards may have to be introduced to regulate the rights and obligations between unitholders of a sidechain. Further, such an investment scheme, may be construed as a collective investment scheme under s 235 of the Financial Services and Markets Act 2000. Such schemes have the following characteristics: a) participants do not have "day-to-day control" of the management of the property,[86] b) contributions of the participants and the profits or income out of which payments are to be made to them are pooled or the property is managed as a whole by or on behalf of the scheme operator.[87] Relating to the requirement of "day-to-day control", Lord Sumption, in the case of *Asset Land v The Financial Conduct Authority*,[88] opined that control of the property meant the ability to "decide what is to happen to it" and this extended to arrangements where the investor would be able to do so.[89] Notably, Lord Sumption held that the investors were not in day-to-day control because there were no arrangements to organise themselves such that they were in a position to control the management of the whole site. Similarly, any peer-to-peer exchange platform built over a blockchain land registry is likely to lack such an arrangement as well.

Even assuming the legislation barring collective investment schemes relating to land is amended to allow for such peer-to-peer exchange platforms, it is questionable whether this will actually increase levels of property ownership.[90] Simply put, given that retail investment in property does not necessarily require ownership of title deeds, having a blockchain land registry customised to allow for fractional ownership of land may not necessarily contribute much by way of allowing retail investors to participate in the property market.

---

83 Vos *et. al.* (n 68) 23.
84 See Paech (n 7) 1088.
85 Statista Research Department, 'First-time buyers: Biggest Barriers to buying first property in the UK 2019' (18 Feb 2020) <https://www.statista.com/statistics/1033495/main-barriers-in-buying-a-first-home-uk/> accessed 7 January 2021.
86 Financial Services and Markets Act 2000, s 235(2).
87 Financial Services and Markets Act 2000, ss 235(3)(a) and 235(3)(b).
88 *Asset Land v The Financial Conduct Authority* [2016] UKSC 17.
89 ibid [94].
90 Bennett, *et. al.* (n 2) 442.

(4) Reducing Fraud

Finally, in a typical land transaction, it is possible for the buyer to present the seller with a forged ownership certificate or with a forged identity. Malviya suggests that this would be a "thing of the past" in a blockchain land registration system,[91] because the use of unique digital ownership certificates in a blockchain land registration system makes it impossible for one to sell or advertise a property one does not own.[92] Indeed, property ownership in a blockchain system is associated with possession of a private key: only the person who possesses the private key can transfer the land token.[93]

While this appears attractive, Barbieri and Gassen highlight the possibility that the private key itself may be lost or stolen.[94] Private keys are generated using code and random number generators, and if done properly, will render the probability of guessing a user's private key all but a statistical impossibility. But the code or random number generator used to generate such code could be faulty, thereby allowing cyber criminals to guess the private key and transfer the land token.[95] It is therefore unclear whether the specific type of fraud identified by Malviya could be reduced by a blockchain land registration system.

(5) Genesis Block Problem

In order to shift the existing Land Registry infrastructure to a blockchain-based land registry system, it is necessary to first identify all of the existing land rights in the Land Registry. This information must then be transcribed (the "**transcription process**") into the first block of the blockchain (the "**Genesis block**"). For a blockchain land registration system to function, the participants of the blockchain system must accept the Genesis block as a suitable starting point. This is dependent on at least two things: (a) first, the reliability of the information in the existing land registry, and (b) secondly, the accuracy of the transcription process.

Vos and others observe that the rights reflected in the land registry may not always be reliable especially when a land registry is corrupt or is of poor quality.[96] In jurisdictions with these land registries, it would be difficult to get participants to accept the Genesis block. Although this limitation may not be applicable to Her Majesty's Land Registry, there is still a risk that the information in the existing Land Registry is inaccurate or incomplete. Therefore, if policymakers decide to adopt blockchain for the purpose of land registration, it may be necessary to institute an insurance policy to indemnify (a) those affected by pre-existing defects in the Land Registry and (b) those affected by errors in the transcription process. Alternatively, amendments may be made to existing legislative provisions, *viz*, schedule 8 of the Land

91 Malviya (n 69).
92 ibid.
93 Maurice Barbieri and Dominik Gassen, 'Blockchain – can this new technology really revolutionize the land registry system?' (World Bank Conference on Land and Poverty, Washington DC, 2017).
94 ibid.
95 Independent Security Evaluators, 'Ethercombing: Finding Secrets in Popular Places' (23 April 2019) < https://www.ise.io/casestudies/ethercombing/> (accessed 7 January 2021).
96 Vos *et. al.* (n 68).

Registration Act which indemnifies persons who suffer loss as a result of rectification of the register to correct a mistake, to cover these types of cases.

(6) 51 Per Cent Attack Problem

As alluded to in Part B, blockchain systems are generally designed to be tamper-evident: it is difficult for rogue participants to introduce falsified records onto the blockchain. Koch and Pieters explain that in order for a rogue participant to fool all of the participants of the blockchain, it has to surpass the work of all the honest participants and create the longest blockchain.[97] This means that it has to (a) edit the particular block it wishes to falsify, and (b) edit all of the blocks that were based on the original, unedited block.[98]

However, a blockchain system is vulnerable if an actor (or a group of actors) manages to control a sufficiently large proportion of the total computational resources held by all the participants in a given blockchain. This is known as a "51 per cent attack", though controlling a simple majority of the network's resources is, while sufficient, not necessary.[99] Barbieri and Gassen explain that a wealthy despot who seizes the majority of the mining power within a blockchain land registry system, thereby snatches the ability to dictate the types of transactions to be included in the blockchain land registry system.[100] This is not a mere theoretical possibility. In July 2014, a bitcoin mining pool acquired over 51% of the network's resources for one day, though no malicious activity occurred.[101] A number of smaller blockchain networks (for which obtaining majority control is simpler) have also fallen victim to such attacks.[102]

While 51% attacks primarily affect POW-based chains (which, to recall, rely on computationally-intensive math problems to enforce immutability), similar vulnerabilities apply *mutatis mutandis* to all POX systems: the attacker need only control a sufficient proportion of X. It is therefore precarious to use any POX-based chain for land registration. Vos and others thus advocate a "hybrid" blockchain for land registration,[103] wherein only authorised entities (e.g. certified conveyancers, notaries and the Registrar) are allowed to upload transactions onto the blockchain. While it is still possible for a consortium of conveyancers to falsify entries on a hybrid blockchain system, the risk could be mitigated with appropriate criminal and civil sanctions. Notice that this is effectively an argument for

---

97 Cristopher Koch and Gina Pieters, 'Blockchain Technology Disrupting Traditional Records Systems' (2017) <https://ssrn.com/abstract=2997588> accessed 7 January 2021.

98 ibid.

99 Recall from Part B that POW is in essence a race to solve a computationally-intensive mathematical problem. The more computational resources one has the easier this is but, as with legal ownership of company shares, one need not always control a simple majority to win, particularly if the remaining resource-holders are dissipated. A simple majority, of course, *guarantees* victory. See Muhammad Saad, *et. al.*, 'Exploring the Attack Surface of Blockchain: A Comprehensive Survey,' in IEEE Communications Surveys & Tutorials, 11-12.

100 Barbieri and Gassen (n 93).

101 Saad, *et. al.* (n 102) 11.

102 ibid, 12.

103 Vos *et. al.* (n 68).

blockchain land registers to be effected on private chains. But this may in turn preclude the possibility of establishing the public peer-to-peer exchange networks described above.

(7) Wide-Ranging Legislative Reform Required

If an exchange platform is to be built over a blockchain land registration system, legislative reform is required. It is necessary to, among other things and at the very least, change the laws relating to formalities in land transactions. The principal statutes setting out the formalities required in land transactions are the Law of Property Act 1925 and the Law of Property (Miscellaneous Provisions) Act 1989.

For example, a contract for the sale or other disposition of an interest in land can only be made in writing and only by incorporating all the agreed terms in one document.[104] In addition, conveyances of land or of any interests therein are generally void unless made by deed.[105] Legal mortgages must also be made by deed.[106] These formality requirements – among others – must be amended to recognise the validity of the transactions on a blockchain land registration system and its exchange platform.

It is also necessary to rethink, for example, the legal remedies associated with a land transaction which is *void ab initio* (*eg* in the case of fraud). Generally, a transaction which is void would be treated in law as if it has not occurred. In a hybrid blockchain land registration system, a court faced with a void transaction could do one of two things (a) order the authorised persons to recognise a transfer of the land token back to the original owner, or (b) order the authorised persons to undo the illegal transfer of land token. Although the latter option is a closer implementation of the legal fiction of *void ab initio*, it would involve re-creating all of the blocks that were based on the affected block. Thus, the latter option may not be practical as it would require serious computing power.

Evaluation

While a blockchain land registry has certain, albeit qualified, advantages, *viz*, data transparency, expediting transactions and reducing fraud, these advantages could easily be realised through a digitised land registry instead. Here, we synthesize the above observations into the following argument against blockchain land registers: private blockchains are far better (in terms of security and compatibility with the current land registration systems) than public blockchains for implementing them, but the advantages afforded by a private blockchain land register can already be, or have already been, realised through digitised land registries.

In addition, we would further observe that while we have illustrated our arguments using the conveyancing system in England as an example, our analysis would be equally applicable to other common law countries, such as Australia or Singapore for two reasons. First, the Land

[104] Law of Property (Miscellaneous Provisions) Act 1989, s 2(1).
[105] Law of Property Act 1925, s 52(1).
[106] Law of Property Act 1925, s 85(1).

Registry, just as it does in England, plays a central role in the conveyancing process. In Singapore, for example, the Land Registry maintains the land register which contains records such as folios of specific parcels of registered land and instruments of dealings registered under the Land Titles Act.[107] The land register is taken to reflect the true state of land ownership,[108] and a registered title, having validity and priority over unregistered interests, can only be challenged on limited grounds.[109] Second, the recognition of equitable land interests,[110] which as we argue below, a blockchain is unable to account for.

Private Over Public Blockchain

The most famous example of a public blockchain would be that of Bitcoin – it began as a permission and trust-less network, but over time, influence from the social and cultural context in which Bitcoin operated slowly seeped in. For instance, block validation has been dominated by a few players for the associated, and highly lucrative, creation of new bitcoins.[111] Thus, the development of the Bitcoin network is effectively controlled by a few entities. Further, the programmers who control Bitcoin's base code play the role of "gatekeepers between user consensus and computer code" thereby giving them more influence than other nodes.[112] Consequently, Bitcoin largely resembles an oligopolistic market structure, a far cry from its initial aspirations. In the context of a public land registry, this would essentially entail transferring control from the Land Registry to the hands of those who a) possess the requisite technical expertise to exert influence over the system and b) those who possess sufficient computing power to control large chunks of the system to create new tokens for users to spend.

Doing so disregards the vital role played by the Land Registrar, whose job involves administering the complex, contentious application which arise when property rights conflict.[113] For instance, in applications made to alter the register,[114] land registry lawyers act as gatekeepers in assessing the viability of arguments made.[115]

There are a few more reasons to prefer a private blockchain over a public one. First, in relation to the 51% attack problem, a private blockchain land registry would be less vulnerable than a public one. A public blockchain becomes susceptible the moment a hacker gains control of 51% of the participants in the blockchain. In contrast, a private blockchain, where only

107 Alvin See, Yip Man and Goh Yihan, *Property and Trust Law in Singapore* (Wolters Kluwer, 2019),93.
108 *Ibid*. This is known as the "mirror principle" under the Torrens system.
109 *Ibid*. This is known as the "indefeasibility principle" under the Torrens system.
110 See *Ho Kon Kim v Lim Gek Kim Betsy and others and another Appeal* [2001] 3 SLR(R) 220 at [25] – [26], *Bahr v Nicolay (No. 2)* (1988) 164 CLR 604
111 Paech (n 7), 1091, citing Primavera De Filippi and Benjamin Loveluck, 'The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure' (2016) 5 Internet Policy Review 7.
112 ibid.
113 John Pownall and Richard Hill, 'The Land Registry's Perspective' in Amy Goymour, Stephen Watterson and Martin Dixon (eds), *New Perspectives on Land Registration, Contemporary Problems and Solutions* (Hart Publishing, 2018) 7.
114 Land Registration Act 2002, s 65 and schedule 4, para 5.
115 Pownall and Hill (n 112) 9.

authorised conveyancers are granted access, is less susceptible given that access to the network is restricted.

Second, as pointed out earlier, one might lose their private key. It is one thing to lose your private key to your bitcoin wallet,[116] and a whole other thing to lose your private key to your land token. In the former, losing a private key would just mean that those bitcoins cannot be spent (i.e. they are lost forever, until one finds the private key).[117] In the latter, that would mean losing the ability to deal with the land in question. This could potentially frustrate any court ordered remedies in relation to land (i.e. specific performance). Another issue that arises is how rectification of title should be carried out on a blockchain land registry. For instance, if a squatter successfully applies for rectification of the register on the basis of adverse possession, the register might possibly be rectified through a court order for the transfer of the private key from the registered owner to the squatter. However, refusal of the registered owner to transfer the private key may frustrate efforts in this regard. While it has been suggested elsewhere that courts can take proactive action to prevent loss of a private key,[118] or invoke the law of contempt to compel the registered owner to transfer the key,[119] it still does not eliminate the possibility that the private key may be well and truly lost. Given this, one can see the necessity of retaining some form of central control to issue a replacement code or an override.[120] This can only be done through a private blockchain.

Third, the blockchain is fundamentally a form of data storage. All parties to the network will always have an updated record of all transactions that have taken place. This might be useful in the context of the financial industry where there is enormous multiplication and diversification of the records of financial assets across jurisdictions.[121] But this feature of blockchain is less relevant in the context of land registry given that there is only one data source maintained by the Registrar. People wishing to check land records simply have to consult the registry. Converting to a public blockchain results in decentralisation when there is no clear need or incentive to do so, especially since having multiple backups would have the same benefit as decentralisation in the event of a hack or destruction of the data storage unit (i.e. having duplicate records stored elsewhere). Moreover, decentralisation also creates additional risks, *viz*, the possibility of a 51% attack.

---

116 Mauro Conti, Sandeep Kumar, Chhagan Lal and Sushmita Ruj, 'A Survey on Security and Privacy Issues of Bitcoin' (2018) 20(4) IEEEE Communications Surveys & Tutorials, 7.

117 ibid.

118 Andrew Hinkes, 'Throw Away the Key, or the Key Holder? Coercive Contempt for Lost or Forgotten Cryptocurrency Private Keys or Obstinate Holders' (2019) 16(4) Northwestern Journal of Technology and Intellectual Property, 256–257.

119 ibid, 257–258.

120 Thomas and Huang (n 8), 24. See also Hinkes, (n 117), 257. Hinkes notes that regardless of proactive measures taken by the court against a contemnor, there is little that can be done to recover truly lost keys.

121 Paech (n 7), 1079.

Private Blockchains – Old Wine in New Bottles?

It would therefore seem that a private blockchain is a feasible model countries could adopt for their land registries. However, many of the advantages proffered by a private blockchain can already be realised through a digitised or electronic land registry for the following reasons.

First, private blockchains allow for greater security by restricting access to the system to authorised users. But existing technology already allows for this. For instance, Australia has modernised its land registry and allowed for electronic conveyancing. At the core of the Australian system, only authorised users such as law firms or financial institutions meeting the criterion set forth in the Participation Rules[122] are allowed to prepare, sign and lodge electronic instruments in the Land Registry.[123] Those applying to use the platform must undergo a stringent process to verify their identity before they are allowed to give a digital signature.[124] Therefore existing technology coupled with stringent requirements for access to the system and penalties for non-compliance may have the same effect as unique digital ownership certificates in a blockchain land registration system.

Second, if one accepts that a private blockchain model is needed, and access is only restricted to registry lawyers and conveyancers, with the registry being granted special powers within the system to make changes where necessary (possible because of the permissioned model of a private blockchain), there is little discernible difference between a blockchain land registry and a digitised one. After all, blockchain is merely a form of data storage, albeit a disintermediated one. This is likely to leave us, in the worst case scenario, with a land registry that is costly, inefficient and not decentralised, and in the best case scenario, an equally efficient alternative to a digital land registry without significant functionality improvements.[125]

And this brings us to our third point. Blockchain, for one, must provide for equitable title in a manner that recognises the interplay between equitable and legal title. One might argue that equitable titles can be stored on a side chain. However, a side chain is separate from the main chain, and transactions made on the side chain do not affect the main chain at all. Blockchains therefore, rather unsurprisingly, do not represent a quantum improvement over existing land registration systems. Interests in land are after all not merely limited to the legal title found on the register. Take for example the facts of *Gallarotti v Sebastianelli*.[126] Sebastianelli and Gallarotti had both contributed money in the ratio of 3:1 towards buying a property, with legal title being registered in Sebastianelli's name. They had an understanding that they would share in the property equally. However, they had a falling out and Gallarotti asked for a court declaration as to his interest in the property. Inferring from the parties' conduct, the court held that their financial contributions should be taken into account in

---

[122] Sharon Christensen, 'Automation of a Torrens register: an Australian perspective' in David Grinlinton and Rod Thomas (eds) *Land Registration and Title Security in the Digital Age* (Routledge, 2020), 216, citing the Model Participation Rules (Australia), r 4.3.
[123] ibid.
[124] ibid.
[125] Schuster (n 5) 18 – 19.
[126] [2012] EWCA Civ 865.

determining their beneficial share of the property. The case demonstrates two points. First, there are equitable interests not listed in the registry. Second, the existence and extent of these equitable interests may only be determined upon a court judgement. This makes the task of ensuring that all equitable interests are also completely listed in the registry difficult. In short, the existence of equitable interests outside of the land register poses exactly the same problem to a blockchain based land registry as it does to conventional land registries.

E. Conclusion

Advancements in technology have precipitated new ways of improving the land registration process through automation. However, at the intersection of law and the potential afforded by technology, it is important to separate fantasy from reality. Examining the characteristics of blockchain shows that a private blockchain would be best suited to the demands of a land registry, however, many of its associated advantages can already be gained through the use of a digitised land registry, sans the new and novel problems implementing such a system would have. While the time has undoubtedly come to modernise land registries through the adoption of technology, modernisation should not be done for the sake of it. Doing so should involve a careful assessment of the characteristics of the proposed technology and whether it is best suited to the demands of a land registry in the 21st century. Instead of attempting to force fit existing land registration systems into the Procrustean bed of blockchain technology, the effort might be better spent in unlocking the full potential of the data stored on a digitised land registry.[127] Naturally, this creates its own set of interesting issues in relation to data ownership and the commercialisation of land registries, and given developments afoot, especially in the deployment of AI and machine learning in the real estate context,[128] we can expect rapid developments in the coming years.[129]

[127] Pamela O'Connor, 'A Broader Development Perspective' in Amy Goymour, Stephen Watterson and Martin Dixon (eds), *New Perspectives on Land Registration, Contemporary Problems and Solutions* (Hart Publishing, 2018), 36.

[128] See The Future of Real Estate Transactions (n 81).

[129] See Sjef van Erp, 'Are land registers becoming online intermediary platforms of land data?' in David Grinlinton and Rod Thomas (eds) *Land Registration and Title Security in the Digital Age* (Routledge, 2020); Bennett, *et. al.* (n 2); and Lynden Griggs and Rouhshi Low, 'Privatisation, the consensus algorithms of blockchains and Land titling in Australia: where are we now, and where are we going?' in David Grinlinton and Rod Thomas (eds) *Land Registration and Title Security in the Digital Age* (Routledge, 2020).