Black Hole Zero-Knowledge Proofs

Melanie Swan, PhD, Philosophy Department, Purdue University

"The only true voyage of discovery is not to visit strange lands but to possess other eyes."
- Proust, *In Search of Lost Time*, Volume V, 1929, 349

Introduction

This essay argues that the AdS/CFT correspondence, as a limits-based lens of undecidability and non-computability, highlights quantum reality as being not only information-theoretic, but rigorously computational as a mathematically-sound domain with built-in cryptographic security features such that black holes provide their own zero-knowledge proofs. The AdS/CFT correspondence (anti-de Sitter space/conformal field theory) is a hypothesis asserting that any physical system with a bulk volume can be described by a boundary theory in one fewer dimensions. The result is that a seemingly complex incomputable system in a chaotic bulk volume is rendered solvable as a boundary theory in one fewer dimensions.

This proposal is in service of the larger task of developing an information-theoretic view of physical reality. The AdS/CFT correspondence is a model propelling scientific advance in many fields, and also a candidate for the kind of theory-building that is necessary to construct an information-based view of reality. Thinkers such as Schrödinger, Von Neumann, Nurse (2008), and Davies (2019) have reflected on the role of information as an instruction set that inherently directs the behavior of physical systems. However, theories that place information on a physical basis or construe a physical theory of information are yet to be defined beyond initial work such as Shannon information theory. Davies distinguishes between the "software" approach to physics based on information theory, instructions, and computability, and the "hardware" approach to physics based on matter, forces, and energy. The implication is that the two approaches should be integrated, putting information theory on a physical basis, and finding a physical theory on the basis of information.

The motivation for this work is to employ limits-based reasoning to address what seems to be a contemporary disconnect between theoretical physics and applied physics. Head-scratching over theoretical problems continues, while simultaneously, there is rapid progress in the implementation of quantum information systems. Commercial quantum computers with superconducting circuits (on-premises and cloud-based) are shipping from three vendors: IBM and Rigetti (controllable gate model superconductors with ~19 qubits) and D-Wave Systems (less-controllable quantum annealing machines with ~2048 qubits).

Advances in quantum computing are having real-life consequences for physics by transforming formerly intractable quantum mechanical problems of undecidability, uncomputability, and unpredictability into analytic solvability. The analytic solvability of quantum mechanical problems is conveyed in two trajectories. One area of advance is the concrete tools of MERA (multiscale entanglement renormalization ansatz) tensor networks which give the ability to solve entangled quantum-many body problems (Vidal 2008, Swingle 2012), and TPU (tensor processing unit) clusters which process complex matrix multiplications of linear algebra without having to store intermediate values in memory. A second vector of advance is conceptual progress in areas such as random tensors (Gurau, 2016), geometric algebra (Hestenes, 1986), and area entropy laws (Bekenstein 1973, Hawking 1975).

Shining the lens of the AdS/CFT correspondence on quantum mechanics reveals that nature's quantum security features provide an even more robust computational domain than was appreciated. These security features include the no cloning theorem, the no measurement principle, error correctability, unique quantum statistical signatures through the SEI properties of quantum objects (superposition, entanglement, and interference), and zero-knowledge proofs (proofs revealing no information except whether the proposition is True or False). The implication is that there is an information-theoretic interpretation of any physical phenomenon, which means a computability, complexity, systems-theoretic, and provability interpretation.

The result of this work is that the AdS/CFT correspondence is demonstrated as a juggernaut formulation that ties together not only physics and information theory in a limits-based computational method as a feature for analyzing problems in contemporary physics, but also incorporates a new level of soundness with cryptographic mathematical properties.

Discovery by Proof of Limitation

Discovery by proof of limitation is a tested method that now comprises a basic element in any toolkit for scientific investigation. At minimum, discerning the limits of what can be proved, computed, or predicted in a particular context helps to define the problem of interest. In the era of data science, many fields have a computational complement (e.g. computational physics, chemistry, biology), in which analyzing the computability of various problem classes is one of the first exercises. Computability limits have become part of the basic machinery of problem solving, and further, the initial point of analysis, for example in selecting a specific approach in quantum computing (fewer gates required for qubitization vs. Trotter Suzuki (Low et al., 2019)).

A standard tool for addressing undecidability and non-computability is the computational complexity schema. Computational complexity refers to the necessary computational resources in time and space to calculate the solution to a problem. The schema is based on the Church-Turing computability thesis which investigates whether a problem is computable, and if so, within a reasonable amount of time. A given problem might fall within any of a dozen or more hierarchical tiers of computational complexity in terms of the computational resources required to calculate the problem's solution. A key focus is whether problems can be solved in polynomial time (a reasonable amount of time).

Information-Theoretic Interpretation of Cosmology

An emblematic victory of the discovery by proof of limitations method is that of Harlow and Hayden's proposal to think about the black hole information paradox in terms of information theory and computational complexity (2013). Initially conjectured by Hawking (1975), the black hole information paradox asks how it is possible for entangled bits of quantum information to radiate out of a black hole. Harlow and Hayden claim that even with a quantum computer, there would not be enough time to calculate information related to the entanglement entropy of an information bit radiating out of a black hole, defeating a counterclaim that it would be possible. The theoretical problem is brought into finer-grained resolution with a computational complexity argument that the class of problems that is solvable with a quantum computer (BQP (bounded-probability quantum polynomial)) is not solvable in this case in a useful amount of time. The important advance of Harlow and Hayden is the suggested link between physics and information theory, and the use of computational complexity to analyze these kinds of problems.

An important property of quantum information bits radiating out of a black hole is that they are entangled. This means that one particle in the entangled pair can be measured to obtain information about the other particle (per the no-measurement principle, a quantum particle itself cannot be measured without damaging it, but its entangled partner can). Thus, an advanced computer such as a quantum computer might be able to model all possible pairs of entangled particles, and determine for any particle radiating out of a black hole whether its entangled partner has already exited or is still in the black hole interior. Such a computational endeavor might indeed be possible, but not within a timeframe that would be quick enough to produce useful information while the particle is radiating out of the black hole, and perhaps not even within the life cycle of the universe.

Quantum Computing allows a One-tier Speed-up in Computational Complexity

Theoretical experiments applying information theory to problems such as the black hole information paradox have led to a refinement of expectations of what is thought to be possible in a potential era of quantum computing. As a gross heuristic, quantum computers may allow a one-tier increase in the computational complexity schema of problem calculation (it is not that all classical problems become solvable). Any problem that takes exponential time in classical systems (too long) may take polynomial time in quantum systems (a reasonable amount of time for practical use). In the canonical Traveling Salesman Problem, perhaps twice as many cities could be checked in half the time using a quantum computer.

Hence, the information-theoretic approach is a wide-ranging paradigm for cosmology research and the understanding of physical reality. The broader implication of Harlow and Hayden is that there is an information-theoretic interpretation of any problem in physics and cosmology, and that the computability of a problem is an important parameter of its resolution.

Exemplar of this kind of linkage between computability and foundational physics is the advent of on-chip laser-driven particle accelerators, which might replace large-footprint traditional accelerators with a 10^4 reduction in scale (Sapra et al., 2020). Using chips only a few inches long, electrons are accelerated using laser light (optical frequencies) instead of radio waves. This involves coupling the laser light, coupling the electrons, and generating fields that are in phase with the electrons. The on-chip accelerator could not be realized with traditional methods, but relies on quantum computation and quantum optical physics to optimize vacuum wave guides and couplers to achieve the desired acceleration.

The AdS/CFT Correspondence

The AdS/CFT correspondence is a further example of discovery by proof of limitation as a model for relating a bulk volume to a boundary surface. The bulk can be described as an anti-de Sitter space, and the boundary as a conformal field theory (a simple field theory). Anti-de Sitter space is a simpler model of the normal de Sitter space of lived reality (de Sitter, 1917).

Practically, the AdS/CFT correspondence hypothesizes that any physical system with a bulk volume can be described by a boundary theory in one fewer dimensions. What seems to be a non-computable bulk volume becomes solvable as a boundary theory in one fewer dimensions. For example, the overall universe could be considered as a bulk volume for which there might be a boundary theory that describes it, in one fewer dimensions. Even without accessing the edge (getting outside of the universe), the correspondence might be applied to derive information about the emergence of bulk structure such as matter distribution, geometry, and time and space.

The AdS/CFT correspondence was introduced as a formalization of the holographic principle, which denotes the possibility of a 3D volume being reconstructed on a 2D surface. Susskind (1995, extending the ideas of 't Hooft) proposed the holographic principle to consider black holes, suggesting a holographic correspondence between the 3D interior bulk and the 2D surface of the event horizon. Black holes are a domain in which the incompatibilities between general relativity and quantum mechanics become more prominent.

The holographic principle argues that there are different but complementary views of the same physical phenomenon. It is known from general relativity that a situation looks different to different observers. Whereas a far-off observer only sees information smearing out or being compressed in 2D on the event horizon of a black hole (the boundary) and never actually entering the black hole (the bulk), a near-by observer that is jumping into the black hole sees the information going into the bulk interior in 3D. Each observer analyzes the black hole per their own stance. The complementary views of observers per the holographic principle (far-off in 2D and near-by in 3D) means that there is no inconsistency, only two different ways of seeing the same physical phenomenon.

Conceiving black holes as a situation of holographic correspondence solves a number of problems about the apparent incompatibilities between the bulk (interior) and boundary (event horizon) regions of the black hole. One puzzle concerns entropy and the finding that black hole interior entropy is different from regular entropy. Black hole entropy scales by area as opposed to volume, whereas "regular" thermodynamic or von Neumann entropy scales by volume. For example, if a room were to be filled with computer hard drives, the amount of information that could be stored is based on the volume of the room, not the area, but in black holes, the entropy is based on the area. The so-called Entanglement Area Law is used to calculate entropy that scales by area as opposed to volume (Bekenstein 1973, Hawking 1975). The holographic correspondence can be used to articulate black hole entropy as a correspondence between the two complementary views of bulk entropy scaling by area and boundary entropy scaling by volume. Subsequently, the Bekenstein-Hawking Entanglement Area Law has been formalized into the Entanglement Entropy Law specific to the Ads/CFT correspondence (Ryu & Takayanagi, 2006).

Probing the limits of black hole entropy led to the formulation of the entanglement area law that black hole entropy scales by area as opposed to volume. An additional finding is that the entanglement area scaling law applies to <u>any</u> quantum mechanical domain, thus having implications beyond black hole physics to quantum systems in general (Eisert et al., 2010). In quantum systems, a general rule applies that entropy scales by area not volume. The immediate consequence of entropy scaling by area not volume is that these kinds of problems are much more easily computable. Area-related problems can be solved in one fewer dimensions than volume-related problems. One practical implication is that the AdS/CFT correspondence can be used to analyze quantum-many body systems in quantum computing. The AdS/CFT correspondence is already being employed to study various phenomena in superconducting materials, condensed matter plasmas, machine learning, blockchains, and network theory.

Maldacena formalized the holographic principle into the AdS/CFT correspondence (1998), subsequently more accurately termed gauge-gravity duality (2012). Gauge-gravity duality suggests that both gauge theories (which describe the behavior of subatomic particles) and gravity have field-related aspects that can be interpreted together in one perspective. The implication of the Ads/CFT correspondence as gauge-gravity duality is the possibility of solving seeming incompatibilities between general relativity (related to gravity) and quantum mechanics (related to particles). One deployment of these ideas is in random tensors which exploit the idea that geometry is comprised of fields which can be computed as matrices (Gurau, 2016). The persistent result is that quantum mechanical domains are becoming more easily computable.

Holographic Error Correction Codes and Quantum Computing

A prominent computability method derived from the AdS/CFT correspondence is holographic quantum error correcting codes, which can be used in quantum computing. Quantum error correction is essential to the realization of quantum computing because quantum information bits (qubits) are more sensitive to environmental damage and decay than their counterpart, classical information bits. Since qubits cannot be easily corrected with a backup copy per the no-cloning rule of quantum information, alternative methods are needed. Quantum error correction is a way of protecting qubits from loss or damage (such as their spin getting reversed). Since quantum bits are entangled with one another, quantum error correction involves embedding qubits into a larger state with an excess of qubits (an ancilla; ancillary or extra qubits) so that even if some qubits are lost, the message can be reconstituted from the entangled qubits.

The AdS/CFT correspondence can be used to define a mapping or holographic code between a logical qubit in a bulk region that needs to be protected, and an entangled ancilla of physical qubits in the boundary that protects it. The mapping or encoding provides a computable dictionary. The error correcting code encodes a single logical spin (in the bulk) in a larger block of physical spins (on the boundary), such that the logical spin is protected against erasure.

For practical implementation, holographic error correcting codes may be instantiated as tensor networks. For example, a holographic code might be a 5-qubit code encoded as a six-leg tensor (Pastawski et al., 2015). The code is represented as a pentagon shape (five-sided) with six tensor legs. A network of the pentagon shapes with six-leg tensors is tiled out to cover a hyperbolic (anti-de Sitter) space. Each pentagon has six tensor legs, one towards the bulk, two towards the neighbors on the left and right, and three towards the boundary. Each tensor has one open leg. The open legs on the bulk are interpreted as the logical input legs of an error-correcting code, and the open legs on the boundary are identified as outputs in which quantum information is encoded. The tensors have bulk-facing and boundary-facing indices. The indices on the tensor legs are differentially contracted and released, with more contraction in the bulk logical space and less contraction in the boundary physical space. This creates a structure for directing the computational flow from the bulk to the boundary to perform the error correction.

The quantum error correcting code engages the natural security features of quantum information in two ways. First, quantum information cannot be accessed locally without damaging or destroying it (per the no-measurement and no-cloning principles). Second, the quantum error correcting code provides the basis for a quantum secret-sharing scheme in that it is based on having a threshold number of participants for reconstitution. Any party holding too few qubits would not have enough information to correct or access the information of the logical qubit, whereas any party or group of parties holding a certain threshold of qubits would have sufficient information about the logical spin. The structure of such secret-sharing schemes is a known mathematical parameter used in the cryptographic security.

Holographic Mapping and Information Compression

The AdS/CFT correspondence, as a form of holographic mapping, is fundamentally an information compression technique, whether enacted as a 3D volume of information smeared out on a 2D black hole event horizon, or as an ancilla of physical qubits in the boundary correcting for one logical qubit in the bulk. Such holographic mapping is also seen in holographic algorithms, which are used for problem simplification (for example, in greater-than-NP hardness problems such as graph theory problems). The technique is to map aspects of a complicated problem to a simpler problem, in a many-to-many relationship among elements.

Holographic mapping provides a higher-dimensional method for compressing the information in the problem. The many-to-many relationships are instantiated with holographic algorithms based on quantum interference patterns (Valiant, 2004). The holographic algorithms generate interference patterns among the solution fragments to the problems at an abstracted level that nevertheless conserves their sum. The holographic algorithms permit reductions in which the specific correspondence (or encoding) between solution fragments of the two problems does not need to remain identifiable. Through the holographic mapping, the information in the problem is compressed such that it can be more easily computed.

Black Holes are Zero-Knowledge Proofs

The link between physics and information theory exposes the natural security features of quantum mechanical domains. These include the no-cloning theorem, the no-measurement principle, quantum error correction through entangled particles, quantum statistics (provable randomness), and the computational complexity class of quantum information (BQP/QSZK). The no-cloning theorem states that quantum information cannot be copied. The no-measurement principle is that quantum information cannot be viewed or measured without changing or damaging it, meaning that eavesdropping is immediately detectable. Quantum error correction is possible through the known entanglement of particles.

Quantum statistics indicates certain distribution signatures that could only have been generated by quantum phenomena. Statistics based on wave function amplitude (interference), entanglement, and superposition could only have been produced by quantum behavior and thus convey provable randomness. The computational complexity class of quantum information (BQP/QSZK) is the computational complexity class of problems that can be solved with a quantum computer. The BQP (bounded-probability quantum polynomial) class is contained within the computational complexity class QSZK (quantum statistical zero knowledge). Zero knowledge refers to the mathematical soundness attribute that it is not necessary to have any knowledge of an underlying process (i.e. zero knowledge), only the result.

Zero-knowledge Proofs

The zero-knowledge concept is used in mathematical cryptography in zero-knowledge proofs. A zero-knowledge proof is a proof that reveals no information other than the correctness of the proposition in question (Goldwasser et al., 1989). The most efficient output of a proof is a one bit answer such as T/F (True/False). Many proofs are inefficient because they contain more information (i.e. knowledge) than is necessary, instead of simply the result of whether the proposition is true or false. One of the easiest ways to construct a proof is to provide a demonstration case, and this was the syntax of many proof structures, for example showing a Hamiltonian tour through a graph as a proof that the graph is Hamiltonian. However, an emphasis on computational efficiency has led to zero-knowledge proofs as a standard technology. An important benefit of zero-knowledge proofs is information security, since having no knowledge (zero knowledge) of the underlying information keeps it private. All that is necessary is the one-bit outcome indicating the truth value of the proof.

Quantum Computational Complexity Domains Perform their own Truth Verification

The zero-knowledge property is implicated in BQP/QSZK in that a traditional prover-verifier relationship (an external verifier) is unnecessary because the quantum computer performs its own truth verification as part of the proof. In these problem classes, the verification can be conducted directly by the computer without the need to engage with a prover who issues a series of interactive queries to test the proof (Watrous, 2002). Quantum computing computes so quickly that it provides a verification of its computation as part of its operation.

The point is that the computational verification capability of zero-knowledge proof technology does not require the involvement of an external verifier. The system provides verification of its result as part of the proof. The computational system serves as a third party, performing truth verification as a feature of the general operation of the system, by relying upon mathematical soundness. Interactive query rounds are outsourced to the computational system, and the accuracy of these checks is itself mathematically checkable. An external verifier can (and should) check the proof output but does not need to engage in an interactive proof process for truth verification.

A real-world analog is a worker punching a time clock every hour and providing the time-stamped records at the end of the day for external confirmation. The supervisor does not need to check the worker's activity every hour, only confirm the oracular (third-party) output of the time punches at the end of the day. Blockchains (automated cryptographic systems for value transfer (Swan, 2015)) implement this kind of non-interactive proof structure. Notable examples are IPFS's (Interplanetary File System) proof of space and time (proof of having provided the space of storage resources over time), cumulatively-verified computationally (Fisch, 2018), and STARKs (Scalable Transparent Arguments of Knowledge (Ben-Sasson et al., 2018)).

STARKs are an oracular proof method in which the prover uses an error-correcting code (Reed-Solomon code) to smooth and encode proof data into an artificial apparatus created for the purpose of the proof. The proof body is an elaborate structure of internal consistencies that fall into place if random queries to it are true, and otherwise evaluates as false (e.g. if an imposter is attempting to submit a fake proof). At the end, the prover sends a summary of the proof body and random verification queries to the verifier, who easily checks its validity computationally.

Holographic Proofs

STARKs are an example of holographic proofs, further demonstrating the reach of the holographic principle and the utility of the AdS/CFT correspondence as a computability method. Holographic proofs are proofs in which every statement contains information about the entire proof. The benefit is that the whole of the proof can be checked with only a few samples. The intuition comes from holography in which it is possible to reconstruct the whole image from any subsection of the image in a laser-generated hologram.

The implication is that quantum computing has zero-knowledge proof technology built into it as a feature. BQP performs its own truth verification. The consequence is that quantum computational systems perform their own truth verification. Black holes, as any quantum computational domain, provide their own zero-knowledge proofs.

Two-Tier Information Systems

The AdS/CFT correspondence and zero-knowledge proofs are indicative of the even bigger class of two-tier information systems. Both the AdS/CFT correspondence and zero-knowledge proofs are two-tier information compression systems, one in time, one in space. The AdS/CFT correspondence is a two-tier information system in that there is a messy complicated area of detailed information and compressed usable information in one fewer dimensions in space (such as the smearing out of 3D information on a 2D plane). Likewise, a zero-knowledge proof does not need the underlying data and only requires a process to run in time to yield the compressed level of information at the end as to whether the proof is True or False. Two-tier information systems are themselves a structure which can be used in exploiting quantum reality, whether in theoretical physics or quantum computation.

Conclusion

As the granular comprehension of physical reality grows, models for its understanding are paramount. This essay argues that the AdS/CFT correspondence constitutes the beginning of an information-based theory of physical reality, and indicates that quantum reality is not merely information-theoretic, but rigorously computational. The AdS/CFT correspondence renders what seems like an impossibility in one dimension - whatever is undecidable, uncomputable, and unpredictable - analytically solvable in another.

The startling premise of the AdS/CFT correspondence is that reality can be computed. Quantum mechanics might remain incomprehensible, but at least it can be computed. The correspondence is a practical tool for activating the quantum realm from the macroscale of lived reality. In some sense, macroscale reality is a surface theory on the messy bulk of quantum mechanics. Higher-dimensional surface theories can be used to direct bulk processes.

Humanity is only just beginning to deploy the kinds of information systems that are more tightly coupled to physical laws. Alignment with quantum mechanical reality is part of the vision proposed by Feynman from the start as the simulation of quantum reality (1982) and the creation of quantum mechanical computers (1985). Thus, quantum computing is the implementation of a technology that is already found in nature, including its full suite of features related to computability limits, security, and mathematical soundness.

Engaging problems of undecidability, uncomputability, and unpredictability yields progress in the positing of an information-theoretic view of physical reality with real-life consequences for foundational physics. As a result, a new theory can be proposed. The Black Hole Zero-Knowledge Theory of Quantum Reality posits that information systems can be employed, the AdS/CFT correspondence in space and zero-knowledge proofs in time, to probe the deeper conceptual questions that remain open in quantum physics and cosmology, for example those related to the existence and emergence of geometrical and dynamical structure, and space and time. The farther stakes of this work are the greater potential for the understanding and manipulation of physical reality.

References

Bekenstein, J.D. (1973). Black holes and entropy. *Phys. Rev. D* 7:2333.

Ben-Sasson, E., Bentov, I., Horesh, Y. & Riabzev, M. (2018). Scalable, transparent, and post-quantum secure computational integrity. ia.cr/2018/046.

Davies, P. (2019). *The Demon in the Machine*. London: Penguin.

de Sitter, W. (1917). On Einstein's theory of gravitation, and its astronomical consequences. Third paper. *Mon. Not. R. Astr. Soc*. 78:3-28.

Eisert, J., Cramer, M. & Plenio, M.B. (2010). Area laws for the entanglement entropy: Review. *Rev. Mod. Phys*. 82:277.

Feynman, R.P. (1982). Simulating physics with computers. *Int. J. Theor. Phys*. 21(6):467-88.

Feynman, R.P. (1985). Quantum Mechanical Computers. *Foundations of Physics*. 16(6):507-31.

Fisch, B. (2018). PoReps: Proofs of space on useful data. ia.cr/2018/678.

Goldwasser, S., Micali, S. & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM J. Comput*. 18(1):186-208.

Gurau, R.G. (2016). *Random Tensors*. Oxford UK: Oxford University Press.

Harlow, D. & Hayden, P. (2013). Quantum computation vs. firewalls. *J. High Energ. Phys*. 2013, 85.

Hawking, S.W. (1975). Particle creation by black holes. *Commun. Math. Phys*. 43(3):199-220.

Hestenes, D. (1986). A Unified Language for Mathematics and Physics. In *Clifford Algebras and Their Applications in Mathematical Physics*. J.S.R. Chisholm; A.K. Commons (eds.). NATO ASI Series (Series C). Springer. 183:1-23.

Low, G.H., Bauman, N.P., Granade, C.E., et al. (2019). Q# and NWChem: Tools for Scalable Quantum Chemistry on Quantum Computers. arXiv:1904.01131.

Maldacena, J. (1998). The large N limit of superconformal field theories and supergravity. *Adv. Theor. Math. Phys*. 2:231-52.

--------. (2012). The gauge/gravity duality. In: G.T. Horowitz (ed.), *Black Holes in Higher Dimensions*. Cambridge UK: Cambridge University Press, p. 32547.

Nurse, P. (2008). Life, logic, and information. *Nature*. 254:424-6.

Pastawski, F., Yoshida, B., Harlow, D. & Preskill, J. (2015). Holographic quantum error-correcting codes: Toy models for the bulk/boundary correspondence. *J. High Energ. Phys*. 6(149):1-53.

Proust, M. (1929). The Captive. *In Search of Lost Time*. Volume V. Trans. C.K. Scott Moncrieff. New York: Random House.

Ryu, S. & Takayanagi, T. (2006). Holographic derivation of entanglement entropy from AdS/CFT. *Phys. Rev. Lett*. 96:181602.

Sapra, N.V., Yang, K.Y., Vercruysse, D., et al. (2020). On-chip integrated laser-driven particle accelerator. *Science*. 367(6473):79-83.

Susskind, L. (1995). The world as a hologram. *J. Math. Phys*. 36(11):6377-96.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Sebastopol CA: O'Reilly Media.

Swingle, B. (2012). Entanglement renormalization and holography. *Phys. Rev. D* 86:065007.

Valiant, L. (2004). Holographic algorithms. In: *FOCS 2004*. Rome, Italy: IEEE Computer Society, October 17-19, pp. 306-15.

Vidal, G. (2008). A class of quantum many-body states that can be efficiently simulated. *Phys. Rev. Lett*. 101:110501.

Watrous, J. (2002). Quantum statistical zero-knowledge. arXiv:quantph/0202111.