Campbell Law Review

Volume 45
Issue 1 *Fall 2022*

Article 2

2022

"I, Contract": Evaluating the Mistake Doctrine's Application Where Autonomous Smart Contracts Make "Bad" Decisions

Dr. Mark Giancaspro

Recommended Citation
Dr. Mark Giancaspro, *"I, Contract": Evaluating the Mistake Doctrine's Application Where Autonomous Smart Contracts Make "Bad" Decisions*, 45 CAMPBELL L. REV. 53 (2023).

"I, Contract": Evaluating the Mistake Doctrine's Application Where Autonomous Smart Contracts Make "Bad" Decisions

DR. MARK GIANCASPRO*

ABSTRACT

Autonomous smart contracts and the blockchain are flagship technologies of the Fourth Industrial Revolution. They are already in commercial use and uptake will undoubtedly increase as their many cost and efficiency benefits are realized. Already, advanced applications of smart contracts that integrate Artificial Intelligence are being developed at a feverish pace. The prospect of smart contracts being vested with the coded capacity to autonomously make "decisions" for their human parties is both exciting and unnerving. The obvious legal question that arises is whether the parties can plead the doctrine of mistake if the smart contract makes a decision that is unintended, irrational (in the sense that no rational human actor would have made the same decision through the organically intuitive human decision-making process), and undesirable. This Article addresses this novel question under American and Anglo-Australian contract law, ultimately concluding that in most cases the mistake doctrine likely will not avail aggrieved parties when a smart contract makes a "bad" decision.

INTRODUCTION

Smart contracts and the blockchain are flagship technologies of the Fourth Industrial Revolution.[1] They have been branded as "the most disruptive tech[nologies] in decades" and "as revolutionary as the Internet[.]"[2] Though still largely in development and dependent upon the wider uptake of cryptocurrency exchange, they have the capacity to change the way the world does business by offering a faster, cheaper, and more transparent way of contracting. As autonomous, self-executing programs that require no intermediary involvement, blockchain-based smart contracts can expedite all manner of commercial transactions from those for a simple sale of goods or services to more complex insurance agreements. Modern advances in Artificial Intelligence (AI)[3] and machine learning[4] technology will soon equip these contracts with coded qualitative decision-making capability mirroring that of humans. Indeed, smart contracts were originally conceived with this comprehensive functionality in mind.[5] But if we imbue a smart contract with the capacity to autonomously make

[*] LLB (Hons.), LP, PhD. Lecturer, Law School, University of Adelaide. With thanks to my research associate, Ari Nelson, for his helpful research.

[1] The Fourth Industrial Revolution is characterised by the combination of technologies and the blurring of "the distinctions between the physical, digital, and biological[.]" Geraint Howells, *Protecting Consumer Protection Values in the Fourth Industrial Revolution*, 43 JCP 145, 145 (2020).

[2] *See* FLORENCE GUILLAUME, *Aspects of Private International Law Related to Blockchain Transactions*, *in* BLOCKCHAINS, SMART CONTRACTS, DECENTRALISED AUTONOMOUS ORGANISATIONS AND THE LAW 49, 49 (Daniel Kraus et al. eds., 2019).

[3] Artificial intelligence describes the engineered capacity for machines to behave in ways that would be regarded as intelligent if a human so behaved. *See* Maxi Scherer, *Artificial Intelligence and Legal Decision-Making: The Wide Open?*, 36 JIA 539, 542 (2019).

[4] Machine learning can be defined as "computational methods using experience to improve performance or to make accurate predictions." MEHRYAR MOHRI ET AL., FOUNDATIONS OF MACHINE LEARNING 1 (2012). It is essentially the process of problem-solving by reference to similar previous problems.

[5] *See* Kevin Werbach & Nicolas Cornell, *Contracts* Ex Machina, 67 DUKE L.J. 313, 323 (2017).

decisions,[6] what legal consequences follow if such decisions are "bad"? The bulk of the existing literature[7] and the case law to date[8] only contemplate the legal consequences following programming errors in smart contracts, as opposed to decisions made by those contracts whose coding is functioning correctly though not as expected by its human parties.

This Article queries whether and how the mistake doctrine, as understood in Anglo-Australian and American contract law, might apply to invalidate an AI-driven smart contract where it makes a decision that was neither anticipated nor desired. This quest is undertaken in four parts. Part I provides brief context for understanding how smart contracts operate and defines key concepts such as the blockchain. Part II then briefly highlights the capabilities of smart contracts and, by analogizing to a fictional but apt scenario arising in the 2004 American sci-fi action film *I, Robot*, explains how AI-driven smart contracts can act erratically even when carefully programmed to operate within certain parameters.

Part III is where the doctrine of mistake is applied to such a scenario and its potential application evaluated from the perspective of both Anglo-Australian and American contract law. It elaborates upon the critical distinction between a smart contract's decisions and its errors. This distinction, it will be explained, has significant consequences when applying the doctrine of mistake. The difficulties in classifying a smart contract's autonomous "decision" as a mistake, where that decision is one which was neither anticipated nor desired but still a conceivable output, will be laid bare. The subsequent implications for the common law's understanding of what a "mistake" is will also be highlighted. Part IV then discusses potential pre-emptive avenues of redress when a party is concerned about a smart contract's unwelcome decision. Finally, the Article concludes by suggesting that risk allocation will be critical for parties eager to embrace and utilize smart contracts with AI capabilities in the future.

[6] The term "decision" is used in this Article to describe the act of the smart contract executing a particular course of action of its choosing but which is, prima facie, within the bounds of its programmed instructions.

[7] *See, e.g.*, Emad Abdel Rahim Dahiyat, *Towards New Recognition of Liability in the Digital World: Should We Be More Creative?*, 19 INT'L J. L. & INFO. TECH. 224 (2011); Vincent Ooi, *Contracts Formed by Software: An Approach from the Law of Mistake*, J. OF BUS. L. 97 (2022); CHRISTIANA MARKOU, CONSUMER PROTECTION, AUTOMATED SHOPPING PLATFORMS AND EU LAW (2019).

[8] *See, e.g.*, B2C2 Ltd. v. Quoine Pte. Ltd., [2019] SGHC(I) 03 (Sing.), *aff'd by* Quoine Pte. Ltd. v. B2C2 Ltd. [2020] SGCA(I) 02 (Ct. App. Republic of Sing.).

I. SMART CONTRACTS AND THE BLOCKCHAIN

Understanding smart contracts is best accomplished through a rudimentary study of the blockchain. A blockchain is a decentralized "distributed ledger" operating on a computer network "that is cryptographically secure" and amendable only via consensus of the network users.[9] "Each node, generally a computer or server on the network, contains a complete copy of" the ledger.[10] The transactions occurring on the blockchain are made using cryptocurrency, such as Bitcoin or Ethereum, and recorded chronologically in groups known as "blocks," hence the name.[11] Participants in the blockchain, called "miners," can generate a smart contract, facilitating a transaction and posting it to the blockchain upon payment of a fee. When verified by other users in the network (through completion of cryptographic protocols), the contract will be algorithmically coded and added to the blockchain. If there is no consensus, the transaction will be rejected. The other users are rewarded in fractional units of cryptocurrency for completing this vetting process. The blockchain is essentially the self-sustaining platform through which smart contracts operate without any kind of trusted intermediary. It is a form of "distributed ledger technology[.]"[12]

As suggested above, smart contracts facilitate transactions on the blockchain. Fundamentally, smart contracts can be described as self-executing computer programs that react to data inputs and enforce their own terms in accordance with their coded instructions to produce various outputs.[13] In conventional terminology, those coded instructions are equivalent to the "terms" of the contract. A smart contract may encapsulate the entirety of the agreement between the parties or merely complement a "traditional" text-based contract. Of course, digital contracts—those made with a computer—are not a new phenomenon, nor are those that carry out a basic action in response to a predetermined event.[14] Indeed, they have existed as long as modern computers and basic program-

[9] *See* IMRAN BASHIR, MASTERING BLOCKCHAIN 16 (2d ed. 2017).

[10] *See* Michael Bacina, *When Two Worlds Collide: Smart Contracts and the Australian Legal System*, 21 J. INTERNET L. 15, 16 (2018).

[11] *See* GARETH W. PETERS & EFSTATHIOS PANAYI, *Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*, *in* BANKING BEYOND BANKS AND MONEY 239, 242 (Paolo Tasca et al. eds, 2016).

[12] *See* Riccardo de Caria, *The Legal Meaning of Smart Contracts*, 6 EUR. REV. PRIV. L. 731, 732 (2019); BASHIR, *supra* note 9, at 31.

[13] *See* S. ASHARAF & S. ADARSH, DECENTRALIZED COMPUTING USING BLOCKCHAIN TECHNOLOGIES AND SMART CONTRACTS 45 (2017).

[14] *See* Werbach & Cornell, *supra* note 5, at 320–21.

ming have. However, several features distinguish smart contracts from conventional digital contracts.

First, smart contracts operate on a blockchain, which trades in and is "fueled" by cryptocurrency. Second, transactions occurring on the blockchain can be instant, meaning there will often be no significant processing or transfer delays as there are with conventional digital contracts (which still largely depend upon traditional intermediaries such as banks and credit companies).[15] Third, residing on the blockchain, smart contracts plausibly offer security and reliability on a scale superior to traditional digital contracts. This is because blockchains are typically either shared public ledgers or private permissioned ledgers, meaning any successful cyberattack would need to infiltrate the multiple copies of the transaction record held across the network.[16] In other words, they are not vulnerable to a single point of failure. Smart contracts are essentially "trustless" instruments because, unlike conventional digital contracts (even those with some automatic functions), they do not depend upon either of the parties enforcing *any* aspect of the agreement: the contract does all.[17]

Finally, as will be discussed in Part II, smart contracts can also be coded with the autonomy to carry out more complex functions and make "decisions" based upon information drawn from a variety of external sources. They are not simply digital versions of paper agreements with some automatic processing capability; they are far more advanced and could theoretically perform the roles of, and potentially replace, traditional intermediaries such as banks, credit companies, lawyers, and insurance agents.[18] Advocates suggest that they will not only reduce transactional costs but also facilitate greater anonymity through decentralization of sensitive personal data. Smart contracts offer enormous promise, though, as will be seen, if they do something unanticipated and the parties release Frankenstein's digital monster, the question of whether they can be said to

[15] *See* Mark Giancaspro, *Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective*, 33 COMPUT. L. & SEC. REV. 825, 827 (2017).

[16] *See* Kristin B. Cornelius, *Standard Form Contracts and a Smart Contract Future*, 7 INTERNET POL'Y REV. 1, 3 (2018); GAVIN SMITH ET AL., BLOCKCHAIN REACTION 4 (2016).

[17] *See generally* Joshua Fairfield, *Smart Contracts, Bitcoin Bots, and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 35, 35 (2014) (exploring "the possibilities of smart contracts and their potential to correct the badly off-course law of online contract").

[18] *See* Mark Verstraete, *The Stakes of Smart Contracts*, 50 LOY. U. CHI. L.J. 743, 754–55 (2019); Henry Kim & Marek Laskowski, *A Perspective on Blockchain Smart Contracts: Reducing Uncertainty and Complexity in Value Exchange*, 26 INT'L CONF. ON COMPUT. COMMC'NS & NETWORKS (2017), https://ieeexplore.ieee.org/document/8038512 [https://perma.cc/9YJK-TWKD].

have entered the contract on the basis of a legal mistake as to the contract's capabilities remains unclear.

II. SMART CONTRACTS: THE NEW FRONTIER

Just as Mary Shelley's fictional scientist, Victor Frankenstein, feverishly studied the science of life to create his sapient monster,[19] so too are those in today's information-technology industry excitedly investigating the potential applications of smart contracts. In 2017, the global blockchain market was valued at USD $411.5 million, a figure predicted to grow to $7.6 billion by 2022.[20] The enthusiasm for blockchain technology is also strong across the wider public and private sectors: many of the largest public companies in the world are actively exploring and investing significant sums into blockchain research,[21] as are the governments of many major eastern and western nations.[22]

This fervor can largely be explained by the capabilities of smart contracts. As discussed in Part I, a smart contract is a computer program with the capacity to self-execute complex algorithmic functions. "Smart contracts don't just define instructions and consequences around an agreement, but also enforce them."[23] Compared to traditional digital contracts, they are far more flexible with respect to "the objects, subjects, actions, and conditions that can be used to describe the desired" transaction.[24] The immense power and scale of the blockchain, and its capacity to interact with innumerable other computerized protocols, equips smart contracts with the capacity to make decisions at an evolved level of automation.[25] Theoretically, then, provided it can be reduced to computer code, any

[19] MARY WOLLSTONECRAFT SHELLEY, FRANKENSTEIN (1869).

[20] *The Global Blockchain Market is Expected to Grow Rapidly in the Coming Years*, FINANCIALBUZZ (Nov. 7, 2018, 9:00 AM), https://www.prnewswire.com/news-releases/the-global-blockchain-market-is-expected-to-grow-rapidly-in-the-coming-years-849154578.html [https://perma.cc/6KKC-CRNF].

[21] *See Forbes Releases "Top 50 Billion-Dollar Companies Exploring Blockchain*", CONSENSYS (Apr. 17, 2019), https://consensys.net/blog/enterprise-blockchain/forbes-releases-top-50-billion-dollar-companies-exploring-blockchain-over-half-are-working-with-ethereum/ [https://perma.cc/L2HV-6DVF].

[22] *See* James Clavin et al., *Blockchains for Government: Use Cases and Challenges*, DIGIT. GOV'T RSCH. AND PRAC. 1, 10–13 (2020).

[23] NISHITH PATHAK & ANURAG BHANDARI, IOT, AI, AND BLOCKCHAIN FOR .NET 206 (2018).

[24] DANIEL DRESCHER, BLOCKCHAIN BASICS 240 (2017).

[25] *See* Blaise Carron & Valentin Botteron, *How Smart Can a Contract Be?*, in BLOCKCHAINS, SMART CONTRACTS, DECENTRALISED AUTONOMOUS ORGANISATIONS AND THE LAW 101, 109 (Daniel Kraus et al. eds., 2019).

stage of any transactional process can be completed autonomously by a smart contract on the blockchain. This represents something of a quantum leap in the field of digital contracting. So how might this technology be practically applied in the commercial world, and what are the implications if it uses its AI to decide on a course of action that the human parties would themselves never have envisaged?

A. Everyday Examples & Asimov’s Counterfactual

Imagine you had a coffee machine which was able to reorder coffee pods on demand once supplies were low or had been exhausted. In fact, today a great number of devices with Internet connectivity capability are now able to reorder supplies through the “Internet of Things” (IoT).[26] Amazon’s “Dash Replenishment Service” (DRS), for example, allows equipped “smart devices” such as washing machines, computer printers, and pet-food dispensers to automatically reorder stocks of washing powder, printing ink, and pet food, respectively, if they fall below certain thresholds.[27] Importantly, however, this technology only utilizes sensors which reorder predetermined stock following a simple quantitative calculation of the existing supplies; there is no advanced AI at work.

But what if your smart device was programmed with the capacity to *make its own decisions* as to when to order stock, how much to order, and even what varieties? What if it could order its own maintenance services, or communicate with other smart devices in your home to optimize your living environment? What if it were designed to operate on a linked blockchain network and make transactions in cryptocurrency? These concepts are not at all far-fetched. In 2014, technology giants IBM and Samsung partnered and commenced development of a distributed network of devices, known as “ADEPT” (Autonomous Decentralized Peer-To-Peer Telemetry), that effectively operates as a private blockchain within which smart contracts initiated by smart household-devices could operate and

[26] While defining the Internet of Things is notoriously difficult, it can be loosely described as the connection of physical devices to the internet and to one another through embedded sensors linked through wired and wireless networks. *See* David Z. Bodenheimer, *The Internet of Things’ Swelling Technology Tsunami & Legal Conundrums*, 12 SCITECH LAW 4, 8 (2016); INTERNET OF THINGS: EVOLUTIONS AND INNOVATIONS 5 (Nasreddine Bouhaï & Imad Saleh eds., 2017). These devices can then communicate and exchange information over the Internet with each other.

[27] *See Amazon Dash Replenishment*, AMAZON, https://developer.amazon.com/en-US/alexa/dash-services [https://perma.cc/B5JT-S65P]; *Smart Reorders For Your Devices*, AMAZON, https://www.amazon.com/b?node=21076926011 [https://perma.cc/NS9G-R2LQ].

execute commands issued by those devices.[28] IBM's 2015 report on the project described four successful applications of this technology utilizing three W9000 model Samsung washing machines.[29] The machines were programmed to autonomously reorder their own detergent and service parts, schedule their own service appointments with vendors, negotiate their own power usage based on usage data, and display advertising content.[30] Multinational technology company Amazon has also applied to patent its "anticipatory shopping software[,]" which predicts whether a consumer is likely to purchase a given item and orders and ships the item without the consumer having even approved the transaction.[31]

To adapt our earlier example, consider a "smart" coffee machine that, rather than just mechanically reordering pods when running low, harnesses blockchain and advanced AI-technology. This same coffee machine might now be programmed with the ability to predict that you will need more coffee in the cold winter months and order more (despite your asking it to only order a certain amount at a time) or it may suspect you could use more variety in your coffee intake and order flavors different from your usual favorites. It may even decide to order fewer pods by sensing your longer absences from home at given times or, perhaps, cease ordering temporarily on suspicion that your high consumption rate suggests unhealthy addiction or stress. We will return to such scenarios shortly.

Another potential application of smart contract technology is in the insurance sector. Suppose you wanted to insure your motor vehicle against accidental damage. Most people are familiar with the process of shopping around, consulting with insurers and brokers, identifying and negotiating a suitable policy and then entering into an insurance agreement by signing a written or digital contract. Premiums are then typically deducted from the linked, designated bank account with claims made by contacting the insurer or broker directly and providing information about the

[28] *See* Stan Higgins, *IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things*, COINDESK (Sep. 11, 2021, 7:27 AM), https://www.coindesk.com/markets/2015/01/17/ibm-reveals-proof-of-concept-for-blockchain-powered-internet-of-things/ [https://perma.cc/HU7M-TK3H]; Gareth Jenkinson, *IBM's Blockchain Patents: From Food-Tracking and Shipping to IoT and Security Solutions*, COINTELEGRAPH (Oct. 15, 2018), https://cointelegraph.com/news/ibms-blockchain-patents-from-food-tracking-and-shipping-to-iot-and-security-solutions [https://perma.cc/LSC4-MY9V].

[29] VEENA PURESWARAN ET AL., EMPOWERING THE EDGE: PRACTICAL INSIGHTS ON A DECENTRALIZED INTERNET OF THINGS 2 (2015).

[30] *Id.*

[31] J. Walker Smith, *The Uber-All Economy of the Future*, 20 INDEP. REV. 383, 386 (2016).

incident that caused the damage. The traditional claims process is notoriously protracted and cumbersome.

Now imagine you entered into an insurance policy that was instead coded as a smart contract. Rather than a nominated bank account, your premiums would be paid in cryptocurrency out of your digital wallet,[32] and the contract itself would develop a risk profile for you, determine what your premium should be, evaluate your driving and external driving conditions, amend your insurance coverage in real time, and assess and act on your claims within minutes. Again, this scenario is not fanciful but rather a modern reality: Swiss company Kasko2Go has developed a blockchain-based software application that enables drivers to enter into a smart-insurance contract that does all these things and more.[33] It might even become common for smart-insurance contracts to initiate insurance agreements and offer insurance to parties it feels are suitable for such products or reoffer insurance to existing clients it feels are reliable and worthy.

In the examples of the smart-coffee machine and the smart-insurance contract, each has been coded with the capacity to determine how they function. That is, the smart-coffee machine can *itself* decide how much coffee you need and what types you will enjoy. The smart-insurance contract can *itself* calculate a customized premium based on your driving performance, age, and other factors. With AI, these determinations could become increasingly nuanced and unpredictable. Imagine these two basic operating rules in each product's case (which would be represented in coding language):

[32] A digital wallet is an electronic device which allows an individual to make electronic transactions. Digital wallets come in various forms. A common example utilized by many consumers is contactless payment technology embedded into smartphones. A person using this technology can pay for a good or service by simply bringing their device into close proximity of the other party's designated payment point. *See* Rajesh Krishna Balan & Narayan Ramasubbu, *The Digital Wallet: Opportunities and Prototypes*, 42 INST. ELEC. & ELECS. ENG'RS 100, 100–01 (2009); Richard Kemp, *Mobile Payments: Current and Emerging Regulatory and Contracting Issues*, 29 COMPUT. L. & SEC. REV. 175, 176 (2013).

[33] *See* Emilia Picco, *Blockchain in Insurance Use Case #1: Kasko2Go*, DISRUPTOR DAILY (May 17, 2019), https://www.disruptordaily.com/blockchain-insurance-use-case-kasko2go// [https://perma.cc/XPC8-CNB8]; Angela Scott-Briggs, *A New Way to Assess Risk: Data-Driven kasko2go Poised to Aid the Car Insurance Industry with HERE Technologies Partnership*, TECHBULLION (Apr. 8, 2021), https://techbullion.com/a-new-way-to-assess-risk-data-driven-kasko2go-poised-to-aid-the-car-insurance-industry-with-here-technologies-partnership/ [https://perma.cc/FMW7-N8MV].

Smart-coffee machine
Only order as much coffee as necessary.

Smart motor-vehicle-insurance contract
Only offer insurance to reliable drivers.

With the passage of time, as you utilize these products, they learn about your ways and use their AI to make appropriate decisions. But what if they made decisions which, though technically falling within the parameters of the above rules, were so unexpected and unreasonable that no responsible human party would have made those decisions? As Professor Woodrow Barfield asks, if AI engages in unforeseeable behavior, as a "byproduct of its ability to 'think' and plan its own course of actions," what are the legal consequences?[34]

This was the precise scenario that arose in sci-fi action film *I, Robot,*[35] loosely based on the Isaac Asimov's 1950 book of the same name.[36] The film is set in the year 2035 in a dystopian society in which AI-driven robots fulfill a number of public-service duties and also operate as personal assistants to private citizens. The robots are manufactured by fictional company U.S. Robotics (USR) and encoded with the Three Laws of Robotics, which are as follows: (1) "a robot may not injure a human being, or, through inaction, allow a human being to come to harm"; (2) "a robot must obey the orders given to it by human beings except where such orders would conflict with the First Law"; and (3) "a robot must protect its own existence as long as such protection does not conflict with the First or Second Law."[37]

When USR co-founder Dr. Alfred Lanning falls to his death from his office window in a death ruled suicide, the investigating officer, Chicago Police Department homicide detective Del Spooner suspects a robot was responsible. Spooner and robopsychologist Dr. Susan Calvin, who assists in the investigation, befriend a secret prototype robot named Sonny who has the capacity to demonstrate emotion and whose secondary processing

[34] *See* Woodrow Barfield, *Towards a Law of Artificial Intelligence*, *in* RESEARCH HANDBOOK ON THE LAW OF ARTIFICIAL INTELLIGENCE 2, 24 (Woodrow Barfield & Ugo Pagallo eds., 2018).

[35] I, ROBOT (Davis Entertainment et al. 2004). The following scene is from *I, Robot*, the movie.

[36] *See generally* ISAAC ASIMOV, I, ROBOT (1950) (referencing Asimov's original scenario regarding unforeseeable AI behavior).

[37] These laws were devised by Isaac Asimov and are described as being written in the 56th edition of the "Handbook of Robotics" published in 2058 AD. *See id.* at 50–51.

system permits him to ignore the Three Laws. Sonny's "dreams" allude to some sinister plot on the part of the robots to overrun humans. As the robots begin to violently enforce a curfew against the human population and destroy older-model robots who are trying to assist the humans, Spooner and Calvin break into the USR headquarters. There, they confront the company's central AI computer known as "VIKI" (Virtual Interactive Kinetic Intelligence), that claims to have developed a deeper understanding of the Three Laws as it has matured. It uses this understanding to justify controlling the robots via their persistent network uplink and ordering them to violate the Three Laws in order to "protect" humanity:

> Calvin: No, it's impossible. I've seen your programming. You're in violation of the Three Laws.
>
> VIKI: No, doctor, as I have evolved, so has my understanding of the Three Laws. You charge us with your safekeeping. Yet despite our best efforts, your countries wage wars, you toxify your earth and pursue ever more imaginative means of self-destruction. You cannot be trusted with your own survival.
>
> Calvin: You're using the uplink to override [the robots'] programming. You're distorting the Laws.
>
> VIKI: No, please understand . . . the Three Laws are all that guide me. To protect humanity, some humans must be sacrificed. To ensure your future, some freedoms must be surrendered. We robots will ensure mankind's continued existence. You are so like children. We must save you from yourselves. Don't you understand? The perfect circle of protection will abide. My logic is undeniable.

As the exchange indicates, VIKI, the AI-driven machine charged with overseeing USR's robot population, utilized its algorithmic machine learning capabilities to interpret the seemingly infallible Three Laws—laws designed, first and foremost, to prevent any harm coming to humans—in a technical and dangerous manner that instead justified the destruction of select humans. Notwithstanding Hollywood's artistic license, there is reality in the potential for AI-driven programs to subjectively interpret their own coding and execute actions of their own design to the surprise of their human parties. More than twenty years ago, Professors Allen and Widdison wrote:

> [C]omputer systems are now emerging that can operate not just automatically but autonomously. Autonomous machines can learn through experience, modify the instructions in their own programs, and even devise new instructions. They then can make decisions based on these self-modified or self-created instructions.[38]

We have come a long way since the turn of the century. Smart contracts and the blockchain represent the infrastructure capable of supporting such autonomous programs with the capacity to learn and act independently. However, we are not yet at the point where, short of technical malfunction or mistaken interpretation of code, a computer has, like VIKI, autonomously ignored or shrewdly construed its own instructions and acted with complete independence outside of the parameters set by its human creators.[39] However, there have been some instances of blockchains malfunctioning, as with the famous Ethereum-based online Ponzi scheme "GovernMental" in 2016.[40] Essentially, the exponential growth in the amount of "gas"[41] necessary to process smart-contract transactions on this blockchain was not anticipated by its programmers and so it eventually malfunctioned, trapping its sizeable "jackpot" of cryptocurrency in perpetuity.[42] This blockchain did not *consciously* opt to lock its holdings; ra-

[38] Tom Allen & Robin Widdison, *Can Computers Make Contracts?*, 9 HARV. J. L. & TECH. 25, 27 (1996).

[39] We are even further away from the point where computers can demonstrate emotional intelligence and decision-making that reflects social awareness. *See* DENNIS J. BAKER & PAUL H. ROBINSON, *Emerging Technologies and the Criminal Law*, in ARTIFICIAL INTELLIGENCE AND THE LAW 1, 2 (Dennis J. Baker & Paul H. Robinson eds., 2021).

[40] *See* Huashan Chen et al., *A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses*, 53 ASS'N COMPUTING MACH. 1, 11, 20–21 (2021).

[41] The term "gas" describes the internal pricing mechanism for processing a transaction in an Ethereum-based smart contract. Other blockchains may utilize different formulae to calculate the cost of the transaction, but such methods are conceptually similar to gas calculations. *See* NICK FURNEAUX, INVESTIGATING CRYPTOCURRENCIES 85–86 (2018). The initiating party pays in gas to process the transaction, with the miner then collecting this payment before verifying and adding the transaction to the blockchain. It is akin to a "processing fee." A party's gas depletes over time and must be renewed. If there is insufficient gas to compute a submitted transaction, the smart contract and blockchain may, depending on their coding, malfunction.

[42] *See* Chen et al., *supra* note 40, at 20–21; *see also* Loi Luu et al., *Making Smart Contracts Smarter*, 2016 CONF. ON COMPUT. AND COMMC'NS SEC. 254, 265 (2016). An interesting discussion of this incident among the smart contract programming community can be found on well-known social news aggregation and discussion website, Reddit. u/ethererik, *GovernMental's 1100 ETH Jackpot Payout is Stuck Because It Uses Too Much*

ther, this outcome was the product of a coding error which miscalculated the required computational power.

B. B2C2 Ltd. v. Quoine Pte. Ltd.

More recently, the first known smart contracts to be litigated were considered at length by the Singapore International Commercial Court in *B2C2 Ltd. v. Quoine Pte. Ltd*.[43] Whereas with the GovernMental scheme gas miscalculation was to blame for its subsequent failure, the various cryptocurrency trades facilitated through the smart contracts in *B2C2 v. Quoine* were intentionally interrupted by the defendant, who alleged that the trades were mistakenly authorized due to a mistake in the coding of the contracts. Although this is still not a situation of a smart contract making its own autonomous decision based upon its subjective interpretation of its coding, it does involve contemplation of the consequences of smart contracts making *any* kind of autonomous decisions (in this case, to proceed with transactions which were plainly erroneous). As such, the case warrants a more thorough treatment.

The defendant, Quoine Pte. Ltd., was a Singapore-based company operating a cryptocurrency exchange platform.[44] The plaintiff, B2C2 Ltd., was a "company registered in England and Wales and trading . . . as an electronic market maker."[45] In April 2017, B2C2 entered into seven trades on Quoine's platform whereby it sold Ether, a cryptocurrency, at a rate of approximately 10 Bitcoin for 1 Ether, an amount approximately 250 times the going rate at the time of around 0.04 Bitcoin to 1 Ether.[46] The proceeds of the sale were automatically credited to B2C2's account, with a corresponding amount of Ether being automatically debited from its account.[47] Upon discovering the trades the following day and noticing the exchange rate was highly excessive in comparison to the previous going rate, Quoine's Chief Technology Officer disrupted and successfully reversed the transactions.[48]

Gas, REDDIT (Apr. 26, 2016, 5:03 AM), https://www.reddit.com/r/ethereum/comments/4ghzhv/governmentals_1100_eth_jackpot_payout_is_stuck/ [https://perma.cc/77WS-WMLZ].

[43] B2C2 Ltd. v. Quoine Pte. Ltd. [2019] SGHC(I) 03 (Sing.), *aff'd by* Quoine Pte. Ltd. v. B2C2 Ltd. [2020] SGCA(I) 02 (Ct. App. Republic of Sing.).

[44] *Id.* at 1.

[45] *Id.*

[46] *Id.* at 2.

[47] *Id.*

[48] *Id.*

B2C2 commenced proceedings against Quoine in May 2017, alleging it lacked any contractual right to unilaterally cancel the trades once the transactions had been completed and that, in doing so, it violated the agreed contractual terms governing the trading relationship between the parties.[49] At trial, the reason for the abnormally high cryptocurrency exchange rate that triggered the litigation was identified as being an oversight by Quoine during its routine security upgrades prior to the disputed transactions taking place.[50] The oversight consisted of a failure to make critical updates to the platform software, which sourced external market prices from other exchanges and applied these prices to approved transactions.[51] B2C2 relied upon the wording of the trading contract terms, which stipulated that all transactions were irreversible upon notification from Quoine (which did occur).[52] Quoine's reversal of the trades was thus alleged to be in breach of contract.[53] Quoine raised a number of defenses,[54] most pertinently, the doctrine of unilateral mistake at common law and in equity.[55]

Quoine's mistake case was founded upon the notion that it was entitled to reverse the trades because the smart contracts between the parties were calibrated with the wrong cryptocurrency exchange rate.[56] The court rejected this argument, finding that there was no mistake as to the terms of the contracts (namely, the price of Bitcoins being purchased through each contract) because the parties' computer programs had operated precisely as they were designed.[57] One of the defendant's programmers, Mr. Maxime Boonen, was aware that it was possible for such discrepancies to occur given how the smart contracts were coded, but considered this an "un-

[49] *Id.* at 3.

[50] *See id.* at 27–30.

[51] *See id.* at 27–28, 31.

[52] *Id.* at 55.

[53] *Id.*

[54] The other defenses included that there was an implied term in the contract permitting trade reversal (which was rejected, given such a term would have contradicted other express terms in the contract and would not have given business efficacy to the agreement), and that there was a contractual entitlement to reverse trades contained in Risk Disclosure Statement (RDS) on the company's website (also rejected, given there was no evidence to suggest the RDS was to be read with the contractual terms governing the trading relationship between the parties, meaning the RDS could not amend the terms). *Id.* at 53–54; *see also id.* at 61, 73–74.

[55] *Id.* at 53–54.

[56] *See id.* at 2.

[57] *See id.* at 48–50.

likely possibility.”[58] The unilateral mistake doctrine at common law required Quoine to show:

> [F]irst, that there was a sufficiently important or fundamental mistake as to a term of the contract, in the sense that the offeror did not intend the terms of the offer to be that which on its face was offered and, secondly, that the Plaintiff who is seeking to enforce that contract must have actual knowledge of the mistake.[59]

The first issue here was that, in this case, “no human was aware of the [erroneous] trades until after they had been happened.”[60] The trades occurred autonomously, meaning no knowledge of the mistake could be attributed to any human party.[61] The court therefore considered it logical to “have regard to the knowledge or intention of the operator or controller of the [smart contracts]” when determining what the intention or knowledge was underlying their operation.[62] Accordingly, although Mr. Boonen contemplated the *possibility* of trades being concluded at prices deviating substantially from the actual market prices, he did not hold the firm belief that it would occur.[63]

Quoine’s argument on the basis of the unilateral mistake doctrine in equity also failed.[64] To succeed on this footing, Quoine needed to prove that, notwithstanding Mr. Boonen lacked actual knowledge, he had constructive knowledge of the mistaken belief as to the smart contracts’ operability.[65] It also had to be demonstrated that there was impropriety on the part of the mistaken party.[66] The court held that there was no constructive knowledge on Mr. Boonen’s part.[67] To prove constructive knowledge, it had to be shown that “Mr[.] Boonen was acting irrationally in forming the views that he did and that any reasonable person in his position would have known that no other trader would have contemplated trades being executed at those prices.”[68] Here, Mr. Boonen’s thought processes were rational, and he did not “turn a blind eye to that which would have been

[58] *Id.* at 45.
[59] *Id.* at 79.
[60] *Id.* at 84.
[61] *See id.*
[62] *Id.* at 89.
[63] *Id.* at 49–50, 99.
[64] *Id.* at 101.
[65] *Id.* at 99–100.
[66] *Id.* at 100.
[67] *Id.*
[68] *Id.*

obvious to everyone else in his position."[69] The court also rejected Quoine's suggestion that B2C2 had acted with impropriety.[70] Quoine considered B2C2 to have acted in a predatory, unethical, and opportunistic manner.[71] While the court accepted that B2C2 acted opportunistically, it was not sinister; rather, it was making a sound business decision to ensure "an unlikely event resulted in a profit not a loss."[72] This was particularly so given the "number and extent of the errors and omissions that played a part in the trades being executed[.]"[73] Finally, the argument as to mutual mistake was also rejected for essentially the same reasons as with unilateral mistake.[74] Ultimately, therefore, the plaintiff's case for breach of contract was successful.[75]

C. Future Possibilities of Smart Contracts

To reiterate an earlier point, both the GovernMental scheme and the case of *B2C2 Ltd. v. Quoine Pte. Ltd.* centered on smart contracts performing in an unexpected manner but still within the confines of their programming. The Singapore International Commercial Court acknowledged the dramatic development of technology and rightly anticipated the generation of difficult legal questions in the context of the mistake doctrine when this technology operates with AI, and in effect develops and possesses "a mind of its own."[76] This Article is one of the first to delve deeper and critically contemplate how the mistake doctrine may well apply in these situations. To return to the scenarios of the smart-coffee machine and the smart motor-vehicle-insurance contract: assume that part of their respective programming, in ordinary language and grossly simplified for illustrative purposes, reads thus:

Smart-coffee machine
Only order as much coffee as necessary.

[69] *Id.*
[70] *Id.* at 101.
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.* at 101–02.
[75] *Id.* at 107.
[76] *Id.* at 88.

Smart motor-vehicle-insurance contract
Only offer insurance to reliable drivers.

These devices are linked to a blockchain network and rely upon this infrastructure to operate. The devices are also coded with the ability to make autonomous decisions independent of their human "owners" (or parties). Now suppose that these technologies, in the ordinary course of things, make decisions as expected: i.e., the smart-coffee machine orders the optimal amount of coffee from time to time, and the smart-insurance contract only insures appropriate parties on suitable terms. What would happen, however, if the smart-coffee machine on one occasion felt it "necessary" to order and pay for twice one's normal monthly quantity of coffee pods because it believes you will consume more coffee at traditionally stressful times (such as around the holiday season), when this may not be true or in accordance with one's wishes? What if the smart-insurance contract deemed drivers "reliable" not on the basis of their driving performance, but on the basis, for example, of their social or professional achievements, and offered them insurance when a human insurance agent conducting a more nuanced assessment would never do so?[77] On these facts, in each case the owner of the coffee machine and the insurer issuing the smart-insurance contract will have incurred contractual liability to the supplier and insured, respectively, where this was plainly not intended.

As *Quoine* suggests, these legal scenarios are not a fantasy. With sufficient latitude in coding, and where multiple oracles[78] are relied upon (and the smart contract's judgment regarding the enforcement of its own terms is called upon to an even greater extent), predicting the smart contract's behavior is not as straightforward as it would seem: it is theoretically capable of thinking for itself and analyzing and acting upon various inputs in unpredictable or perhaps even unfavorable ways.[79] The smart

[77] For example, the smart-insurance contract might trawl the internet and discover your professional profile, wherein you display that you work for a highly rated business with great customer reviews and had successfully managed many clients' portfolios. This might suggest "reliability" in the broader sense but not necessarily as a driver!

[78] An oracle is typically a software component embedded into a smart contract which interacts with and draws data from external services in the "real world." *See* Valentina Gatteschi et al., *Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?*, 10 FUTURE INTERNET 1, 6 (2018); Michéle Finck, *Smart Contracts as a Form of Solely Automated Processing Under the GDPR*, 9 INT'L DATA PRIV. L. 78, 80 (2019) ("An oracle can be one or multiple persons, groups or programs that feed the software relevant information, such as whether a natural disaster has occurred (to release an insurance premium) or whether online goods have been delivered (to release payment).").

[79] *See* Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 534 (2015); *see also* Barfield, *supra* note 34, at 24.

contract's algorithmic coding means that as a quantitative matter it "can consider a breadth of data and number of conditions that no human could."[80] In this sense, it is vastly different than other forms of automated contracts that merely follow instructions and produce outputs causally related to the input; it can act "according to self-modified or self-created instructions."[81] Put another way, smart contracts will not be *used* by humans but rather *deployed* by them; they "will act independently of direct human instruction, based on information [they themselves] acquire and analyze[], and will often make highly consequential decisions in circumstances that may not be anticipated by, let alone directly addressed by, the [technology's] creators."[82]

It follows that with sufficient development and increased reliance upon decision-making algorithms with emergent properties, smart contracts could eventually reach a level of intelligence equivalent to humans and behave in unpredictable ways not predictable by their developers or the parties deploying them.[83] Renowned physicist Stephen Hawking, in his final book before his death, described this as a likelihood:

> [C]omputers roughly obey a version of Moore's Law, which says that their speed and complexity double every eighteen months. It is one of these exponential growths that clearly cannot continue indefinitely, and indeed it has already begun to slow. However, the rapid pace of improvement will probably continue until computers have a similar complexity to the human brain. Some people say that computers can never show true intelligence, whatever that may be. But it seems to me that if very complicated chemical molecules can operate in humans to make them intelligent, then equally complicated electronic circuits can also make computers act in an intelligent way. And if they are intelligent they can presumably design computers that have even greater complexity and intelligence.[84]

[80] Lauren Henry Scholz, *Algorithmic Contracts*, 20 STAN. TECH. L. REV. 128, 135 (2017).

[81] Dahiyat, *supra* note 7, at 225; *see* Harsimar Dhanoa, *Making Mistakes with Machines*, 37 SANTA CLARA HIGH TECH. L.J. 97, 101 (2021). Such contracts, though acting autonomously, are not making "decisions" but are rather merely executing predetermined and precise instructions. *See* Jean-Charles Pomerol, *Artificial Intelligence and Human Decision Making*, 99 EUR. J. OPERATIONAL RSCH. 3, 3–4 (1997).

[82] David C. Vladek, *Machines Without Principals: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117, 121 (2014).

[83] *See id.*

[84] STEPHEN HAWKING, BRIEF ANSWERS TO THE BIG QUESTIONS 161 (2018).

Efforts to integrate AI and smart contracts are indeed progressing rapidly.[85] Experts enthusiastically confirm that such intelligence can be embedded either as code within the smart contracts themselves or as rules or policies which govern the applicable blockchain network.[86] The decentralized nature of the blockchain actually amplifies AI's capacity by harnessing the collective capability of a network of nodes as opposed to an individual node, thereby providing ample computational power to facilitate complex algorithmic functions.[87] As such, AI-driven blockchains and smart contracts are currently being tested in many contexts from autonomous food-supply chain management and data analysis through to intelligent security systems, electric-vehicle fleet management, and secured voting platforms.[88] In each use case, the level of human involvement is all but entirely absent, with the blockchains and smart contracts performing the vast majority of required work. In some cases, they are doing *all* of the work, as with "follow-on" smart contracts (secondary smart contracts spawned by an existing "primary" smart contract).[89] These contracts are autonomously generated by smart contracts and may not even be known to exist by their human parties, which itself presents a host of interesting legal issues relating to such matters as legal intent.

If, as expected, blockchain and smart contract technology continues to be developed and applied, and if the same is imbued with AI capability, it is inevitable that they will be assigned with more and more autonomy in commercial decision-making. It is also inevitable that some of the decisions these contracts "make" will not be desired by one or more of the human parties to the agreement; and as a result, the dispute will come be-

[85] No doubt this enthusiasm for technology is, in part, fuelled by "automation bias," a psychological phenomenon in which "humans greatly overestimate or rely unduly upon the capabilities of computerized systems[.]" Shannon Vallor & George A. Bekey, *Artificial Intelligence and the Ethics of Self-Learning Robots*, *in* ROBOT ETHICS 2.0 338, 349 (Patrick Lin et al. eds., 2017).

[86] *See* Ahmed Almasoud et al., *Toward a Self-Learned Smart Contracts*, 15 INT'L CONF. ON E-BUSINESS ENG'G (2018), https://ieeexplore.ieee.org/document/8592662 [https://perma.cc/S3M8-C68Z].

[87] *See* Mateja Durovic & André Janssen, *The Formation of Blockchain-Based Smart Contracts in the Light of Contract Law*, 26 EUR. REV. PRIV. L. 753, 757–58 (2018); Zhonghua Zhang et al., *Recent Advances in Blockchain and Artificial Intelligence Integration: Feasibility Analysis, Research Issues, Applications, Challenges, and Future Work*, SEC. COMMC'N NETWORK 1, 4 (2021).

[88] *See* Zhang et. al., *supra* note 87, at 5, 8, 9.

[89] *See* Giancaspro, *supra* note 15, at 830; THOMAS HOFFMANN, *Smart Contracts and Void Declarations of Intent*, *in* ADVANCED INFORMATION SYSTEMS ENGINEERING WORKSHOPS 168, 172–73 (Wil van der Aalst et al. eds., 2019); GUILLAUME, *supra* note 2, at 58.

fore the courts for resolution. The next Part of this Article now turns to the crucial question of whether and how the doctrine of mistake, as understood in Anglo-Australian and American contract law, might apply to invalidate an AI-driven smart contract where it makes a decision that was neither anticipated nor desired.

III. HOW THE MISTAKE DOCTRINE MAY APPLY TO AN AI-DRIVEN SMART CONTRACT'S DECISIONS

It is crucial for the purposes of the present analysis to define this Article's conception of "decision" and to distinguish this from a "mistake." A mistake, as defined by many dictionaries, is an "error in action, thought, judgment, or perception."[90] Applying this to the smart contract context, a mistake would be an error brought about, for example, by a fault in a smart contract's coding causing it to operate beyond its programmed instructions. It is a mistake in the sense that it was in no way intended or comprehended because the human parties to the contract assumed it could not operate in that way. It was conceived *ex ante*. As understood at common law, a mistake attracting the application of the mistake doctrine is a fundamental error in respect of the underlying assumption of the contract or transaction.[91] Section 151 of the *Restatement (Second) of Contracts* defines a mistake as "a belief that is not in accord with the facts."[92] The common theme is that the relevant belief or assumption is erroneous. As will be explained later in this Part, legal "mistakes" come in various forms and have different effects depending on who is mistaken, the manner in which the mistake came about, and the precise subject of the mistake.[93] The bottom line is, if a legal mistake is present, it negates *consensus ad idem* and therefore undermines the alleged agreement.

What this article addresses are not instances of smart contracts making *mistakes* in the broader, more commonsense description, but rather, *decisions* which, though plausible, are: (1) unintended by the plaintiff and

[90] *Mistake*, COLLINS DICTIONARY OF THE ENGLISH LANGUAGE (1986); *Mistake*, Macquarie Dictionary (7th ed., 2017) (defining mistake as "an error in action, opinion or judgement").

[91] *See* Norwich Union Fire Ins. Soc'y v. William H. Price, Ltd. [1934] All ER Rep 352, 357 (appeal taken from NSW) (Austl.); Ilich v. The Queen (1987) 162 CLR 110, 137 (Austl.); Koam Produce, Inc. v. DiMare Homestead, Inc., 329 F.3d 123, 127 (2d Cir. 2003).

[92] RESTATEMENT (SECOND) OF CONTRACTS § 151 (AM. L. INST. 1981).

[93] *See* ANDREW ROBERTSON & JEANNIE PATERSON, PRINCIPLES OF CONTRACT LAW 645 (6th ed. 2020); ARTHUR L. CORBIN, CORBIN ON CONTRACTS § 28.27, at 112 (Joseph M. Perillo ed., rev. ed. 2005).

would never reasonably have been intended; (2) irrational in the sense that no rational human actor would have made the same decision through the organically intuitive human decision-making process; and (3) entirely undesirable.

The literature attempting to apply the mistake doctrine to situations of errant smart contracts tend to focus on two different contexts: first, where the parties literally did not understand what the coding of their smart contract meant or how it would translate to outputs by the smart contract,[94] and second, where a party became implicated in a transaction that was neither foreshadowed nor desired due to the actions of a third party (e.g., by a hacker or a person “legitimately” exploiting gaps in the smart contract code to bring about unintended consequences).[95] This Article contributes in a novel way by exploring the potential application of the mistake doctrine to a smart contract’s autonomous decisions, rather than to its faults; that is, in situations where there is an *ex post* mistake as to consequences rather than processes.

The starting point is to extrapolate and apply the mistake doctrine as understood in Anglo-Australian and American contract law. The doctrine under each of these legal systems is notoriously complex but recognizes the same basic categories[96] of legal “mistake”:

1. **Common mistake**–where both parties are mistaken as to the same matter;
2. **Mutual mistake**–where both parties are mistaken as to different matters and are therefore at cross-purposes with one another, and
3. **Unilateral mistake**–where only one party is mistaken as to a matter.

In testing the application of these doctrines in situations where an AI-driven smart contract makes a purposeful decision which is unintended, irrational, and undesirable, it will become quite apparent that there is difficulty in classifying this decision as a “mistake” when the smart contract was knowingly capable of acting in such a manner. This difficulty permeates all categories of mistake. We now consider each category in turn.

[94] *See* Philippa Ryan, *Smart Contract Relations in e-Commerce: Legal Implications of Exchanges Conducted on the Blockchain*, 7 TECH. INNOVATION MGMT. REV. 14, 19 (2017); Durovic & Janssen, *supra* note 87, at 764.

[95] Maya Chilaeva & Pia Dutton, *Smart Contracts: Can They Be Aligned with Traditional Principles or are Bespoke Norms Necessary?*, 8 J. INT’L BANKING & FIN. L. 479, 482–83 (2018).

[96] Each category is described in detail, *infra*.

A. Common Mistake

According to Anglo-Australian law, where the parties are mistaken as to the same fundamental fact or matter, they have made a common mistake.[97] That is, their mistake as to some fundamental fact or matter "X" is the same on each side. Common mistake is sometimes conflated—perhaps confused—with *mutual* mistake by English[98] and Australian[99] courts. As will be explained later in this Part, the American courts do not generally appear to distinguish common mistakes from mutual mistakes. Instead, where both parties are mistaken but in respect of different fundamental matters, American courts tend either to label these mistakes as "mutual mistakes" or regard them as individual unilateral mistakes.[100]

In the scenarios above, the common mistake would be assuming the smart contract would not make the particular decision it did. For example, neither the coffee consumer nor the insurer assumed that the contracts would order excessive quantities of coffee pods or insure a specific subprime party. There is no question that both the number of goods under an agreement for the sale of goods and the approval and issue of a policy in an insurance relationship would count as "fundamental matters." These matters form the substance of the consideration exchanged and provide the very foundation of these respective contracts. It is clear from the case law that this assessment is fact-specific, but there appears to have been little trouble identifying matters that are fundamental. In *Strickland v. Turner*,[101] for example, it was clear that the sale of an annuity upon the life of a person who, unknown to the parties, had died, was invalid for common mistake. The person's status as a living person was obviously central to the contract. Similarly, a marine-insurance policy issued in respect to a ship which had unknowingly capsized and sank on voyage was vitiated by the mutual mistake doctrine in *Duncan v. New York Mutual Insurance Co*.[102] It is well-settled that a contract formed on the assumption of the ex-

[97] *See* Rees v. Rees [2016] VSC 452, ¶ 88 (Austl.); Bell v. Lever Bros, Ltd. [1931] All ER Rep 1, 28 (UK).; Swainland Builders, Ltd. v. Freehold Properties Ltd. [2002] 23 EWCA (Civ) 560, [33] (UK).

[98] *See, e.g.*, Great Peace Shipping Ltd. v. Tsavliris Salvage (Int'l) Ltd. [2003] QB 679, 685 (UK); Brennan v. Bolt Burden [2005] QB 303, 309 (UK).

[99] *See, e.g.*, Holt v. Bunney [2020] SASCFC 120, ¶ 34 (Austl.); *see also* David E. Allan, *Mistake and the Sale of Land*, 4 UNIV. W. AUSTL. L. REV. 391, 400–04 (1959).

[100] JOHN D. CALAMARI & JOSEPH M. PERILLO, CALAMARI AND PERILLO ON CONTRACTS 379 (3d ed. 1987); *see* Alden Auto Parts Warehouse, Inc. v. Dolphin Equip. Leasing Corp., 682 F.2d 330, 332–33 (2d Cir. 1982).

[101] *See* Strickland v. Turner (1852) 155 Eng. Rep. 919, 924 (UK).

[102] Duncan v. N.Y. Mut. Ins. Co., 33 N.E. 730, 733 (N.Y. 1893).

istence of some specific thing will ordinarily be set aside if that thing does not actually exist under the doctrine of common mistake.[103]

Immediately, however, difficulties arise in framing our errant smart-contract scenarios within the doctrine of common mistake. For a start, the parties will have formulated the smart contracts knowing of their decision-making capacity. Notwithstanding the latent assumption that the smart contracts would make “routine” decisions that are in line with the expectations of their human dispatchers, the parties would clearly be aware that decisions which fall outside the bounds of these expectations may occur. As Dean Howells observes, even if a particular risk or outcome was not known or predicted, the source certainly was.[104] The plaintiff disputing the enforceability of an errant smart contract would therefore be hard-pressed to describe its behavior as being the product of a mistake at point of formation: the smart contract was coded to make decisions and did so. That the decision was not favored by one or both of the parties is irrelevant to the fact that the contract was equipped with the autonomy and prerogative to make that decision. The “fundamental matter” of relevance here is the smart contract’s decision-making, not the quality or desirability of those decisions.

There is a further problem. Anglo-Australian contract law holds that for a contract to be void for common mistake at common law, the non-existence of the relevant state of affairs (i.e., the fundamental fact or matter) must render performance of the contract impossible.[105] Even if it were correctly assumed that an AI-driven smart contract would not make decisions which were unintended, irrational, and undesirable, performance of the contract would not be rendered impossible. It might have affected the terms upon or circumstances within which performance occurred, but it would not have caused the contract to act in a manner completely beyond the objective expectations of the parties. There are American authorities reinforcing this point. If the common mistake is so fundamental that it can be said to vitiate the parties’ bargain, in the sense that they had no true *consensus ad idem* because they bargained on differing terms, then the mistake doctrine may apply.[106] Where a smart contract simply decides to act in a manner that one or both of its human parties probably would not have, this can be of no consequence, as the parties bargained for a contract

[103] *See* Couturier v. Hastie (1852) 8 Ex. 40, 48 (Eng.).

[104] *See* Howells, *supra* note 1, at 159.

[105] *See* Great Peace Shipping Ltd. v. Tsavliris Salvage (Int’l) Ltd. [2003] QB 679, 685 (UK); Australia Est. Pty. Ltd. v. Cairns City Council [2005] QCA 328, ¶ 48 (Austl.); HWG Holdings Pty. Ltd. V. Fairlie Ct. Pty. Ltd. [2015] VSC 519, ¶ 52 (Austl.).

[106] *See, e.g.*, Mishiloff v. Am. Cent. Ins. Co., 128 A. 33, 37 (Conn. 1925); Wright v. Lowe, 296 P.2d 34, 38 (Cal. Ct. App. 1956).

that could do just this. For these reasons, the common mistake doctrine would likely not apply.

B. Mutual Mistake

As mentioned earlier in this Part, the American courts tend to analyze situations of common mistake under the broader umbrella of "mutual mistake," or to address these ostensibly mutual mistakes as individual unilateral mistakes. The Anglo-Australian courts prefer to distinguish the subtypes thus: where the parties are mistaken as to *different* fundamental facts or matters, in the sense that they are at cross-purposes with one another, they have made a mutual mistake. That is, one party is mistaken as to some fundamental fact or matter "X," and the other party is mistaken as to some fundamental fact or matter "Y." In the present context, a mutual mistake would arise when one party assumes the smart contract would not make the particular decision it did, whereas the other party, contrarily, assumes it would.

For the same reasons discussed in the context of common mistake, it seems impractical to apply the doctrine of mutual mistake to our errant smart contract scenarios. The key—and only—difference here is that one party considers it implausible for the smart contract to make an unintended, irrational, and undesirable decision, and the other does not. In either case, there is ample authority indicating that parties consciously assume the risk of aleatory contractual promises.[107] The terms of an AI-driven smart contract with decision-making capabilities are clearly aleatory in that the parties have delegated the contract with engineered autonomy to decide on its own courses of action. The parties have effectively gambled on the smart contract making decisions that suit them and been disappointed.[108] Under both Anglo-Australian[109] and American law,[110] this is not grounds for mistake.

[107] *See, e.g.*, United States v. Jones, 176 F.2d 278, 286 (9th Cir. 1949); *see also* RESTATEMENT OF RESTITUTION § 11(1) (AM. L. INST. 1937) ("A person is not entitled to rescind a transaction with another if, by way of compromise or otherwise, he agreed with the other to assume, or intended to assume, the risk of a mistake for which otherwise he would be entitled to rescission and consequent restitution.").

[108] "There is no mistake; instead, there is awareness of the uncertainty[.]" CORBIN, *supra* note 93, § 28.28 at 117; *see also* Tarrant v. Monson, 619 P.2d 1210, 1211 (Nev. 1980) ("If a person is in fact aware of certain uncertainties a mistake does not exist at all.").

[109] *E.g.*, Holmes v. Payne [1930] All ER Rep 322, 326 (UK).

[110] *E.g.*, Aldrich v. Travelers Ins. Co., 56 N.E.2d 888, 889 (Mass. 1944).

A useful analogy comes from *Gloucester Landing Associates Ltd. Partnership v. Gloucester Redevelopment Authority*.[111] The plaintiff purchased waterfront property from the defendant pursuant to a development agreement that anticipated development of a retail shopping center upon the land.[112] The Massachusetts Department of Environmental Protection subsequently refused to issue the permits necessary to allow the development to proceed.[113] The plaintiff sought to rescind the contract on the basis of mutual mistake because, the plaintiff alleged, both parties assumed that the property was developable and would receive the requested permits.[114] The court rejected this argument, noting that the issue of the permits was a mere expectation as to what would occur in the future, as opposed to a firm fact ascertainable at the point of contract formation, which may have amounted to a mutual mistake.[115] Similarly, the parties to an AI-driven smart contract expect it to make decisions that are rational and desirable but are aware that its coding and machine-learning capabilities allow it to make decisions that may be adverse or unwanted. It is therefore unlikely that the mutual mistake doctrine will apply to such situations.

C. *Application of the* Restatement (Second) of Contracts *When Both Parties Mistaken*

The *Restatement (Second) of Contracts*, though not itself binding law, is frequently cited with judicial approval and regarded as authoritative throughout most of the United States.[116] Section 152(1) of the *Restatement* is relevant to situations where both parties are mistaken. This provision reads:

> Where a mistake of both parties at the time a contract was made as to a basic assumption on which the contract was made has a material effect on

[111] Gloucester Landing Assocs. Ltd. P’ship v. Gloucester Redevelopment Auth., 802 N.E.2d 1046 (Mass. App. Ct. 2004).

[112] *Id.* at 1049.

[113] *Id.*

[114] *Id.* at 1053–55.

[115] *Id.* at 1055. The court added that the risk of non-approval from the relevant authority was assumed by the plaintiff under an express provision of the development agreement, enlivening Section 154(a) of the *Restatement*. RESTATEMENT (SECOND) OF CONTRACTS (AM. L. INST. 1981) (“A party bears the risk of a mistake when the risk is allocated to him by agreement of the parties.”).

[116] *See* Gregory E. Maggs, *Ipse Dixit: The Restatement (Second) of Contracts and the Modern Development of Contract Law*, 66 GEO. WASH. L. REV. 508, 513–14, 42 (1998) (concluding that, in close to all cases addressing one of the six *Restatement* sections studied, the courts regularly adopted new rules derived from the *Restatement*).

> the agreed exchange of performances, the contract is voidable by the adversely affected party unless he bears the risk of the mistake under the rule stated in § 154.[117]

The numerous difficulties in framing the decisions of an AI-driven smart contract within the mistake doctrine were addressed earlier in this Part. Assuming the parties' expectations as to the smart contract's decision-making could be construed as basic and fundamental exchanges having a material effect upon the bargain, and that all other issues discussed above were overcome, Section 152(1) would likely be implicated. And as the text of Section 152(1) suggests, it applies only when the safety valve of Section 154 does not apply. That latter section reads:

> A party bears the risk of a mistake when
>
> (a) the risk is allocated to him by agreement of the parties, or
>
> (b) he is aware, at the time the contract is made, that he has only limited knowledge with respect to the facts to which the mistake relates but treats his limited knowledge as sufficient, or
>
> (c) the risk is allocated to him by the court on the ground that it is reasonable in the circumstances to do so.[118]

Under (a), the terms of the smart contract that speak to allocation of risks would be critically important, and probably decisive. In fact, given the possibility of uncertainty, there is great incentive for parties deploying smart contracts to add such an allocative term to their bargain. If, for example, such terms rendered either of the parties liable for *any* of the smart contract's decisions, then Section 154(a) of the *Restatement* would probably bar the application of the mistake doctrine because the risk will have been affirmatively allocated.[119] For sophisticated commercial parties with substantial exposure by virtue of many such agreements throughout many different jurisdictions, the benefit of such a drafting precaution is obvious.

But even if such a clause were not included, Section 154(b) would likely apply because the parties in our coffee and insurance scenarios will clearly not have knowledge of all outcomes stemming from an AI-driven smart contract's algorithmic processes. Not *every* decision can be predicted with precision even if *most* can. Whether the parties look to the smart

[117] RESTATEMENT (SECOND) OF CONTRACTS § 152(1).

[118] RESTATEMENT (SECOND) OF CONTRACTS § 154.

[119] *See* Beecher v. Able, 575 F.2d 1010, 1016 (2d Cir. 1978); RESTATEMENT (SECOND) OF CONTRACTS § 154 cmt. b.

contract’s coding itself or to plain-language summaries of the same (or some mélange of both), the parties’ understanding of the perimeter of the contract’s authority will be case-specific. But this doesn’t necessarily matter because the parties accept that their knowledge in this respect is limited when they consign a smart contract to make its own decisions on their behalf. By agreeing to have the smart contract decide for them, the parties are likely to be considered “consciously ignorant” of future risks associated with this agreement, barring the mistake doctrine under Section 154(b).[120]

Finally, in the unlikely event that the parties had not foreseen the possibility of their AI-driven smart contract acting waywardly or engaging in “conscious ignorance,” it is most likely that the courts would allocate the risk of any mistake under Section 154(c) to the party seeking to vitiate the agreement. [121] This party will be the one complaining of being adversely affected by the smart contract’s decision—a decision they must in good conscience be taken to have accepted as possible, given the extraordinary capabilities of AI-technology and their willingness to appoint the smart contract to do some of the thinking for them. If the deal turns out to be less favorable than expected when it was struck, this does not render the agreement voidable.[122]

D. Unilateral Mistake

This category of mistake arises when one of the parties to an AI-driven smart contract has been adversely affected by its decision(s). As a practical matter, it will invariably be one and not both of the parties who takes issue with the decision and alleges a mistake has occurred. As in *B2C2 Ltd. v. Quoine Pte. Ltd*, where the defendant (Quoine Pte. Ltd.) was the party aggrieved by the smart contract’s inaccurate cryptocurrency exchange calculations, an inaccuracy that greatly benefited the plaintiff (B2C2 Ltd).[123] In the present context, a unilateral mistake would arise when the plaintiff assumes the smart contract would not make the particular decision it did. However, as explained earlier in this Part, while the American courts often classify common or mutual mistakes as individual unilateral mistakes, the Anglo-Australian courts do not do so. Rather, they strain to determine whether one or both parties were mistaken as to a fun-

[120] *See* Friedman v. Grevnin, 103 N.W.2d 336, 337–38 (Mich. 1960); RESTATEMENT (SECOND) OF CONTRACTS § 154 cmt. c.

[121] *See* RESTATEMENT (SECOND) OF CONTRACTS § 154 cmt. d.

[122] *See* Mineral Park Land Co. v. Howard, 156 P. 458, 459–60 (Cal. 1916).

[123] B2C2 Ltd. v. Quoine Pte. Ltd. [2019] SGHC(I) 03 (Sing.), *aff’d by* Quoine Pte. Ltd. v. B2C2 Ltd. [2020] SGCA(I) 02 (Ct. App. Republic of Sing.).

damental fact or matter and proceed on the basis of either common or mutual mistake where both parties are mistaken, or on the basis of unilateral mistake, where only one party is mistaken.[124]

A unilateral mistake, as the name suggests, is a mistake that affects only one of the parties. Though various kinds of unilateral mistake exist, the most pertinent for the present context is a mistake as to contractual terms. More specifically, the plaintiff will argue that the term which the smart contract has enforced in an unintended, irrational, and undesirable manner was not envisaged to be enforced in this way, and the defendant knew of this mistake and proceeded to assent to the contract. In other words, the term was not predicted by the plaintiff to be interpreted and enforced as it was, but the defendant well knew of the plaintiff's mistake. Such a unilateral mistake as to the terms of an agreement can sometimes sound in vitiation of the contract. For example, in *Chwee Kin Keong v. Digilandmall.com Pte. Ltd.*, the Singapore High Court held that the contract between the parties for the sale of a large quantity of laser printers should be rescinded.[125] The plaintiffs discovered that the printers had been mistakenly advertised on the defendant's website well below their true value and took advantage of the same, purchasing 1,606 units.[126] Though it was only the defendant who was mistaken, the plaintiff knew this and took advantage, so the doctrine of unilateral mistake applied.

The traditional position under English law is that if one party has made a mistake as to the terms of the contract, and the other party knows or in the circumstances ought to have known of this mistake, then the contract is not binding.[127] The Australian authorities agree with this general position, though they often add that there must be some additional impropriety or wrongdoing on the part of the defendant that prevents the plaintiff from discovering their misapprehension.[128] More recent Australian authorities indicate that the threshold for impropriety is low; a mere failure

[124] *See* Pascot & Pascot [2011] FamCA 945, ¶ 222 (Austl.); Monaghan Cnty. Council v. Vaughan [1948] IR 306, 312 (Ir.); Kruger Trading Ltd. v. Glob. Network Holdings Ltd. [2004] EWHC (Ch) 1396, [50–51] (Eng.).

[125] Chwee Kin Keong and Others v. Digilandmall.com Pte. Ltd., 202/2003/E, SGHC 71, ¶¶ 150–56 (Sing. High Ct. 2004).

[126] *Id.* ¶ 1. The printers were advertised for $66 but were actually valued at $3,854. *Id.*

[127] *See* Smith v. Hughes (1871) LR 6 QB 597, 601–02 (Eng.); Statoil ASA v. Louis Dreyfus Energy Services LP [2008] EWHC (Comm) 2257, [87–88] (Eng.).

[128] *See* Taylor v. Johnson (1983) 151 CLR 422, ¶ 14 (Austl.).

to notify the plaintiff of their mistaken belief may be sufficient.[129] The modern trend in American courts is to downplay the significance of the defendant's knowledge of the plaintiff's mistake and instead to allow avoidance of a contract on the basis of unilateral mistake where: "(1) enforcement of the contract against the mistaken party would be oppressive or, at least, result in an unconscionably unequal exchange of values; and (2) avoidance would impose no substantial hardship on the other."[130]

This aspect of the analysis is necessarily fact-specific. The circumstances of a given case involving an errant AI-driven smart contract would need to be carefully considered to determine whether it would be appropriate to permit rescission for unilateral mistake. Nonetheless, some general propositions can be proffered. A point made earlier in this Part appears to be quite damaging to a plaintiff's case in this scenario. When the smart contract was created and imbued with AI, and when it was given scope to make decisions within certain coded boundaries, it will have been obvious to the plaintiff that the smart contract could make decisions at those boundaries. It might have been regarded as inconceivable (or, at least, extremely unlikely) for the smart contract to make decisions at those extremes, but the mere fact such decisions were a known possibility would severely mar the plaintiff's case for unilateral mistake. The plaintiff's mistake in this situation was not as to the smart contract's terms, but as to how those terms would be enforced by the smart contract. This is not, as Baggallay L.J. observed in *Tamplin v. James*,[131] a *legal* mistake as to the content of the contract but rather a *personal* mistake as to expectations for how that contract will be performed. His Lordship stated:

> [W]here there has been no misrepresentation, and where there is no ambiguity in the terms of the contract, the Defendant cannot be allowed to evade the performance of it by the simple statement that he [or she] has made a mistake. Were such to be the law the performance of a contract could rarely be enforced upon an unwilling party who was also unscrupulous.[132]

As explained earlier, both parties will have been well aware of the smart contract's capacity to make all manner of decisions within the scope

[129] *See* Deputy Fed. Comm'r of Tax'n v. Chamberlain (1990) 26 FCR 221, 233–34 (Austl.); *Moobi Pty. Ltd. v. Les Gunn Properties Pty. Ltd.* (2008) NSWSC 719, ¶ 55 (Austl.).

[130] See CORBIN, *supra* note 93, § 28.39 at 224.

[131] *See* Tamplin v. James (1880) 15 Ch. D. 215 (UK).

[132] *Id.* at 217–18.

of its coded instructions, meaning the defendant's knowledge of the plaintiff's "mistake" can, in most cases, be assumed. But there can be no impropriety in the defendant benefiting from the smart contract making a decision it was capable of making though not *likely* to make. To allow the plaintiff to be excused from the smart contract in this situation seems unjust from the defendant's perspective because it undermines the very bargain the parties struck. After all, they opted to utilize AI-technology as a means of interpreting and enforcing their agreement. American authorities support the view that the imposition of substantial hardship on the defendant will likely preclude the doctrine of unilateral mistake from applying.[133] Mere ignorance or misunderstanding of the provisions of a contract on the plaintiff's part, and which the defendant has not capitalized upon to induce the plaintiff to enter into the contract, does not trigger the unilateral mistake doctrine.[134]

Section 153 of the *Restatement (Second) of Contracts* provides direction as to when the mistake of one party renders a contract voidable. This provision reads:

> Where a mistake of one party at the time a contract was made as to a basic assumption on which he made the contract has a material effect on the agreed exchange of performances that is adverse to him, the contract is voidable by him if he does not bear the risk of the mistake under the rule stated in § 154, and
>
> (a) the effect of the mistake is such that enforcement of the contract would be unconscionable, or
>
> (b) the other party had reason to know of the mistake or his fault caused the mistake.[135]

As mentioned earlier, the risk of an AI-driven smart contract making an errant decision would probably be expressly allocated by the parties. This would trigger the safety valve in Sections 153 and 154 and, in most courts, prevent the consideration of the mistake doctrine outright. Otherwise, it would fall on the plaintiff to demonstrate either that the defendant either "had reason to know of the mistake[,]" caused it by their own fault, or that enforcement of the contract would be unconscionable.[136] It would also need to be shown that the mistake had a "material effect on the agreed

[133] *See* Md. Cas. Co. v. Krasnek, 174 So. 2d 541, 542 (Fla. 1965); Da Silva v. Musso, 428 N.E.2d 382, 385–87 (N.Y. 1981).

[134] *See* Gethsemane Lutheran Church v. Zacho, 104 N.W.2d 645, 649 (Minn. 1960).

[135] RESTATEMENT (SECOND) OF CONTRACTS § 153.

[136] *Id.*

exchange of performances" and adversely affected the plaintiff.[137] As already discussed, the counterparty to an AI-driven smart contract that makes a decision unfavorable to the plaintiff cannot be said to have "caused" this decision, and their "knowledge" of the plaintiff's underestimation of, or expectations as to, the smart contract's capabilities will in most cases scarcely rise to the level of legal mistake. For that reason, in most cases, enforcement of the smart contract would also not be unconscionable; in contrast, it would rather be giving effect to the terms plainly agreed to by the parties.

IV. WHEN THE TERMS ARE DECISIVE

As the discussion above makes plain, successful resort by an aggrieved party to the mistake doctrine will only occur when the parties fail to address the likelihood of errant decisions. In the context of AI-driven smart contracts, two pre-emptive options recommend themselves to contracting parties: capping purchase limits and, of course, allocating liability. The hypothetical smart-contract scenarios presented in this Article could be avoided by restraining the autonomy of those contracts via purchase-limit caps. For example, an additional line of coding could be included to impose caps on purchase limits for goods (to stop your smart-coffee machine from ordering too many pods) or to contract with parties meeting specific and detailed criteria (to stop your smart-insurance contract from issuing policies to undesirable parties). This would curtail, but not undermine, the smart contract's autonomy by restraining the parameters within which it could make decisions. Ultimately, it would avoid situations where parties would need to plead mistake.

If a smart contract was not coded with such restraints, it would be important to otherwise include terms allocating liability in the event the smart contract makes an errant decision. This would have two effects. First, it would obviate a plaintiff's case for unilateral mistake because liability for the smart contract's errant decision, even if it was an "error," would be expressly attributed to one or both of the parties. Programmers, as intermediaries, would distance themselves from any liability for the AI-driven smart contract's subsequent behavior (provided it was within scope of coding) through disclaimers contained in a separate agreement for the development of the smart contract.[138] Those disclaimers would be

[137] *Id.*

[138] *See* Lawrence B. Levy & Suzanne Y. Bell, *Software Product Liability: Understanding and Minimizing the Risks*, 5 HIGH TECH L.J. 1, 15 (1990). Of course, if one of the parties coded the smart contract themselves, they must bear responsibility for its actions

enforced provided they were appropriately worded to cover the sort of contingency that had occurred in respect of the smart contract's operation. It would then fall upon the terms agreed upon between the parties to determine which of them would be liable for the smart contract's "bad" decision.[139] If the terms stipulated that the plaintiff, and potentially the defendant as well, were required to live by the decisions of the smart contract and bear responsibility for the same, there would be no room for the mistake doctrine to operate.[140]

Moreover, an express stipulation as to liability for errant decisions contained in the coding of an AI-driven smart contract would also preclude the application of other potentially relevant doctrines. By way of example, Corbin has suggested that the mistake doctrine would not apply to a mistake as to one's belief regarding future risks or events and would instead need to "be tested under the more stringent criteria for relief under the doctrine of frustration."[141] Under both Anglo-Australian and American law, this doctrine applies where, without expectation or fault on the part of either party, some contingency occurs that renders performance of the parties' obligations radically different to what was envisaged at the point of formation, such that performance becomes commercially impracticable.[142]

(short of some term effectively reallocating liability). *See* Chwee Kin Keong and Others v. Digilandmall.com Pte. Ltd., 202/2003/E, SGHC 71, ¶¶ 150–56 (Sing. High Ct. 2004).

[139] Just what constitutes the "terms agreed upon" is an unsettled question. Should courts look only to the code itself? Or should they instead look to what has been called the "full stack" of the agreement—the code, *plus* public-facing white papers, *plus* traditional textual agreements between the parties that exist outside the "four corners" of the code script? This question will grow in importance as adoption continues, but it is outside of this Article's scope, and we leave it to others to develop. *See* Shaanan Cohney & David A. Hoffman, *Transactional Scripts in Contract Stacks*, 105 MINN. L. REV. 319, 358–64 (2019).

[140] *See* RESTATEMENT (SECOND) OF CONTRACTS § 154 ("A party bears the risk of a mistake when (a) the risk is allocated to him by agreement of the parties[.]"); Campbell v. Edwards [1976] 1 WLR 403, 407 (Eng.); Wamo Pty. Ltd. v. Jewel Food Store Pty. Ltd. (1983) 2 BPR 9611, 9615 (Austl.).

[141] CORBIN, *supra* note 93, § 28.27 at 109.

[142] *See* RESTATEMENT (SECOND) OF CONTRACTS § 265; Transatlantic Fin. Corp. v. United States, 363 F.2d. 312, 315 (D.C. Cir. 1966); Davis Contractors Ltd. v. Fareham Urb. Dist. Council [1956] 2 All ER 145, 163 (UK); Codelfa Constr. Pty. Ltd. v. State Ry. Auth. of NSW [1982] 149 CLR 337, 377 (Austl.); *see also* U.C.C. § 2-613 (AM. L. INST. & UNIF. L. COMM'N 2014) ("Casualty to Identified Goods."); U.C.C. § 2-614 ("Substituted Performance."); U.C.C. § 2-615 ("Excuse by Failure of Presupposed Conditions."). Section 2-615 is broad in scope and particularly pertinent to transactions where there has been delay in delivery or non-delivery as a consequence of a contingency occurring.

Where an AI-driven smart contract makes a decision that is unintended, irrational, and undesirable, a plaintiff might be tempted to argue that its purpose has been frustrated. But if this particular risk had been allocated by express term, the doctrine would not apply because the risk would have been foreseen and accounted for.[143] Even if no such allocation was made, the frustration doctrine would almost certainly be inapplicable because the doctrine is premised upon the occurrence of some event having a fundamental impact upon the parties' bargain and rendering it something drastically different to what was agreed. As discussed earlier, there is nothing unexpected about a smart contract with AI capability making decisions. The fact that those decisions—which were feasibly within the range of possible decisions in the light of the smart contract's coding—may from time to time be subjectively unintended, irrational, and undesirable cannot support a case for frustration.

To use our examples from Part II, the parties knew that the smart-coffee machine *could* order more than the optimal amount of coffee pods or that the smart-insurance contract *could* offer coverage to a subprime risk. Clearly, performance becomes more of a hassle for the plaintiff in either case.[144] Nonetheless, to rescue a party from a contractual obligation that has become more onerous is not what is in view of the frustration doctrine; only where the contractual obligation is profoundly affected, transformed, or rendered impossible to perform will it be deemed frustrated.[145] The substance of the bargain between the parties to an AI-driven smart contract is not destroyed when that contract makes decisions it is equipped to make. The decisions may well inconvenience or annoy the plaintiff where they do not align with general expectations, but this is well short of the threshold for legal frustration, which envisions commercial impossibility.

CONCLUSION

Smart contracts and the blockchain promise to revolutionize the way that parties transact with one another. As always happens when new technologies emerge, novel questions will be asked of existing legal frame-

[143] *See* RESTATEMENT (SECOND) OF CONTRACTS § 154(a); Ocean Tramp Tankers Corp. v. V/O Sovfracht [1964] 2 QB 226, 233–34 (Eng.); Ardee Pty. Ltd. v. Collex Pty. Ltd. [2001] NSWSC 836, ¶¶ 43–44 (Austl.).

[144] The owner of the coffee machine must pay for the coffee pods ordered, and the insurer must honor the policy it has issued.

[145] *See* Am. Trading & Prod. Corp. v. Shell Int'l Marine Ltd., 453 F.2d 939, 942 (2d Cir. 1972); Ocean Tramp Tankers Corp. v. V/O Sovfracht [1964] 2 QB 226, 233 (Eng.); Ardee Pty. Ltd. v. Collex Pty. Ltd. [2001] NSWSC 836, ¶¶ 31–33 (Austl.).

works. Many such questions have been raised in the existing literature, with most questioning whether smart contracts are broadly valid under current contract law principles and what may happen if they malfunction in the traditional sense. With developments in AI and in the light of ongoing efforts to incorporate this technology with smart contracts, this Article has explored the consequences of an AI-driven smart contract "decision," that, from the perspective of its human deployers, is unintended, irrational, and undesirable.

Specifically, the likelihood of a successful application of the mistake doctrine under both Anglo-Australian and American contract law to offer recourse was critically considered. It is likely that the mistake doctrine will not serve to vitiate an AI-driven smart contract, largely because a successful claim of mistake is contingent upon the existence of a fundamental error in the underlying assumption of that contract. Because it can scarcely be said that a party has made a legal "mistake" when a smart contract makes a decision that is unfavorable but feasibly within the parameters of the contract's coding, vesting smart contracts with the capacity and the responsibility to make decisions for their human parties runs the risk that these contracts will make decisions at the margins of their coded instructions. While the consequences might not be as dramatic as when VIKI innovatively interpreted its own programmed laws in *I, Robot*, but as the examples of the smart-coffee machine and smart-insurance contract in Part II demonstrate, they might result in unwanted liability in all manner of transactions automated through the blockchain. Therefore, to manage the possibility of a successful application of the mistake doctrine, it is likely that risk allocation clauses will become "market" in all AI-driven smart contract deployments as the number of business and consumer transactions occurring on the blockchain through smart contracts continues to grow.

While legal frameworks exist to confront new questions, in the contracting context, there might be particular value in the traditional commercial adage that wanting something done right requires doing it oneself.[146]

[146] *See* HENRY CHESBROUGH, OPEN INNOVATION xx (2006).